Volume 9, No. 2
June 2011
ISSN: 1545-679X

INFORMATION SYSTEMS EDUCATION JOURNAL

In this issue:

EDSIG
Serving Information Systems Educators

The **Information Systems Education Journal** (ISEDJ) is a double-blind peer-reviewed academic journal published by **EDSIG**, the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is quarterly. The first year of publication is 2003.

ISEDJ is published online (http://isedjorg) in connection with ISECON, the Information Systems Education Conference, which is also double-blind peer reviewed. Our sister publication, the Proceedings of ISECON (http://isecon.org) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the ISEDJ journal. Currently the target acceptance rate for the journal is about 45%.

Information Systems Education Journal is pleased to be listed in the 1st Edition of Cabell's Directory of Publishing Opportunities in Educational Technology and Library Science, in both the electronic and printed editions. Questions should be addressed to the editor at editor@isedj.org or the publisher at publisher@isedj.org.

2011 AITP Education Special Interest Group (EDSIG) Board of Directors

INFORMATION SYSTEMS EDUCATION JOURNAL

Editors

ISEDJ Editorial Board

Are Password Management Applications Viable? An Analysis of User Training and Reactions

Mark Ciampa
mark.ciampa@wku.edu
Western Kentucky University
Bowling Green, KY 42101 USA

Abstract

Passwords have the distinction of being the most widely-used form of authentication—and the most vulnerable. With the dramatic increase today in the number of accounts that require passwords, overwhelmed users usually resort to creating weak passwords or reusing the same password for multiple accounts, thus making passwords the weakest link in the chain of security. It has been recognized that instead of solely relying on their memory for passwords, users can take advantage of technology. One such technology is a password management application, which enables a user to create and store multiple passwords in a strongly protected file and then retrieve them as necessary, thus alleviating the need to memorize numerous passwords. However, few users have chosen to take advantage of these applications. Is it because users have rejected them as poor solutions, or because they were unaware of these applications and their potential benefits? Would users be more favorable towards password management applications after they received training about these applications and then used them? What limitations of these applications could be addressed to foster more widespread use? To-date no studies have provided training to users regarding these applications prior to surveying their reactions to determine if indeed these applications are suitable for the average user. This paper describes a study regarding user's training, use, and perceptions of a password management application.

Keywords: information security, passwords, password management applications, KeePass

1. INTRODUCTION

Authentication is the process of providing proof that a user is actually who they say that they are (Pastore & Dulaney, 2006). Authentication systems are based on the use of a physical token (something you have), a physical characteristic (something you are), or secret knowledge (something you know) that can uniquely distinguish a user (Burnett & Kleinman, 2006). The most common type of authentication in use today is a password (Kruger, Steyn, Medlin, & Drevin, 2008), which is based on something that is only known by the user and thus prevents imposters from impersonating the user.

Yet, despite their widespread use, passwords provide a weak degree of protection and undermine the system (Gaw & Felten, 2006). Schneier (2004) says that "systems are only as secure as the weakest password".

The weakness of passwords centers on human memory. Human beings can memorize only seven (plus or minus two) "chunks" of information (Miller, 1956). As more items are added to memory, the number of items that are forgotten increases (Neath, 1998).

Passwords place heavy loads on human memory in two ways. First, a password should be of a sufficient length and complexity that an attacker cannot easily determine it. However, long and complex passwords of this type can be difficult to memorize and can strain the ability to accurately recall them. Most users have difficulty remembering these types of strong passwords (Charoen, Raman, & Olfamn, 2008).

Second, the number of different accounts and passwords that are required today also places a load on a user's memory. Typically users have multiple accounts for different computers at work, school, and home, for various e-mail accounts, for online banking and Internet sites, to name a few, and each account has its own password. Despite research by Gaw and Felten (2006) showing that the majority of 49 undergraduate test subjects had three or fewer passwords, other studies have indicated a much higher number of passwords per user. Research cited by Vu, Proctor, Bhargav-Spantzel, Tai, Cook, and Schultz (2007) indicated that 35% of users had 3-4 passwords, 18% had 5-6 passwords, 6% had 7 to 8, and 23% of users had 9 or more passwords, while other research showed that 28% of a group had over 13 passwords each. Sasse and Brostoff reported that a group of 144 users had an average of 16 passwords (Sasse & Brostoff, 2001), while Brown, Bracken, Bracken, Zolccoli and Douglas (2004) reported a group of college students (n=218) averaged 8.18 passwords each. Choren, Raman and Olfamn noted that because users have multiple accounts requiring multiple passwords, it is "more than slightly impossible" for users to remember each password (2008).

The problem is even exacerbated by security policies in which passwords are set to expire after a period of time, such as every 45 days, and a new one must be created. Some security policies even prevent a previously used password from being recycled and used again, forcing the user to repeatedly memorize multiple new passwords for multiple accounts.

Due to the burdens that passwords place on human memory, users typically take shortcuts to help them recall their passwords. The first shortcut is to use a weak password. These may include a common word used as a password (such as "January"), a short password (such as "ABCDE"), or personal information in a password (such as the name of a child or pet). The second shortcut is to reuse the same password for multiple accounts, making it easier for an attacker who compromises one account to be able to access multiple other accounts. Research by Gaw and Felten (2006) showed that users accumulate more online accounts, as they get older, yet the number of unique passwords does not increase. As users accumulate more online accounts they are simply reusing passwords more frequently.

Schneier summarizes the issue by stating, "The problem is that the average user can't and won't even try to remember complex enough passwords to prevent dictionary attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it on a Post-it and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications" (2004).

2. ADDRESSING PASSWORD WEAKNESSES

In order to address the weaknesses associated with passwords, different solutions have been proposed to help users overcome poor password practices. These solutions may be grouped into four broad categories.

Change how passwords are created

The first category is comprised of solutions to change how textual passwords are created. Bunnell, Podd, Henderson, Napier, and Kennedy-Moffat (1997) and Yan, Blackwell, Anderson and Grant (2004) have explored rates for different methods to generate and associate text-based passwords. Other researchers have proposed splitting a textual password into two parts: one part is written down on a paper while the second part is encoded in a mnemonic sentence (Topkara, Atallah, & Topkara, 2007).

Substitute graphical passwords

The second category of solutions is substituting textual passwords with graphical passwords. There are three advantages to graphical passwords. Graphical passwords are based on the premise that figures or images are easier for users to recall than text. Also, graphical passwords utilizing images are more difficult for an attacker to circumvent. Finally, graphical passwords may also help address a fundamental weakness of user-created textual passwords, namely that users select passwords that represent themselves and even sum up the very essence of their being in a single word (Gaw & Felten, 2006). Attackers frequently attempt to guess a textual password by using personal information about the user, which could be more difficult with a graphical password.

Proposals for graphical passwords include clicking on specific points of a scene in a particular sequence within an image (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005) or identifying a series of random art images (Dhamija & Perrig, 2000). Another proposal requires the user to identify specific faces (Tari, Ozok, & Holden, 2006). Users are provided a random set of photographs of different faces, typically three to seven, and are taken through a "familiarization process" that is intended to imprint the faces in the user's mind. A user must select his assigned faces from three to five different groups, with each group containing nine faces, before being authenticated. Even using personalized hand-drawn "doodles" for authentication has been proposed by Goldberg, Hagman and Sazawal (2002), Govindarajulu and Madhvanath (2007), and others.

Use alternative authentication methods

The third category of solutions for overcoming weaknesses associated with passwords is to use alternative methods of authentication. One common method is standard biometrics, which uses a person's unique characteristics for authentication and usually involves fingerprints, faces, hands, irises, or retinas. However, because standard biometrics requires a biometric hardware scanning device to be installed at each computer where authentication is required and because of the large numbers of false negatives of rejecting authorized users, standard biometrics have not been widely implemented.

To address the weaknesses in standard biometrics, a new type of biometrics known as behavioral biometrics is being developed. Instead of examining a specific body characteristic, behavioral biometrics authenticates by normal actions that the user performs. Two types of behavioral biometrics are keystroke dynamics and voice recognition. Keystroke dynamics attempt to recognize a user's unique typing rhythm by using two unique typing variables: dwell time, which is the time it takes for a key to be pressed and then released, and flight time, or the time between keystrokes. Voice recognition uses the unique characteristics of a person's voice for authentication. Voice recognition is not to be confused with speech recognition, which accepts spoken words for input as if they had been typed on the keyboard.

Make use of technology

The final category for addressing password weaknesses is to use technology. Modern Web browsers such as Firefox and Microsoft's Internet Explorer (IE) contain a function to allow a user to save a password that has been entered while using the browser (called an AutoComplete Password in IE) or through a separate dialog box that "pops up" over the browser (called an HTTP Authentication Password in IE). AutoComplete passwords are stored in the Microsoft Windows registry and are encrypted with a key created from the Web site address while HTTP Authentication Passwords are saved in the credentials file of Windows, together with other network login passwords.

Another solution in this category for addressing password weaknesses is password management applications. Called the "digital equivalent" to a written Post-It note by Gaw and Felten (2006), these programs let a user create and store multiple strong passwords in a single user file that is protected by one strong master password. Users can retrieve individual passwords as needed by opening the user file, thus freeing the user from the need to memorize multiple passwords.

Yet most password management applications are more than a password-protected list of passwords and include many additional features (Reichl, 2010). One additional feature of many password management applications is the ability to create strong random passwords through random seeding based on a user's mouse movement and random keyboard input. This enables these password managers to meet the criteria for effective password management as set forth by Kruger, Steyn, Medlin, and Drevin (2008) of both creating secure passwords and protecting the confidentiality of them. Examples of password management applications include KeePass, Password Safe, RoboForm, Access Manager, and others.

3. OVERVIEW OF THE STUDY

Despite the advantages of password management applications, relatively few users have chosen to use them. In a study by Gaw and Felten (2006), 49 users were told to bring "anything you use to help you remember your passwords (password lists, daily planners or notebooks, digital assistants, copies of bank or travel statements, copies of items in your Internet browser cache, etc.)". Only six participants brought aids, none of which was a password management application. Gaw and Felten (2006) concluded that these applications "interrupt the user's behavior" and were "relatively unpopular". However, they also stated that "technology solutions could help".

This study sought to determine the reason why password management applications are used so infrequently. Is it because users are familiar with them yet have rejected them as poor solutions, or is it because they are unaware of these applications and their benefits? If the latter is the case, would users be more inclined to use these applications once they received training and actually used them? If not, what are the limitations of these applications that could be addressed to create more widespread use?

Participants

The ideal study population is all users who have passwords. Because that obviously is not possible, a sample was selected that did not cause any serious threats to the external validity. A relatively large sample of undergraduate student participants is representative of that population. Kruger et al. notes that modern universities, with their core business focused on teaching and research, are in fact managed and operated along the same line as any business. In addition, there are a large number of confidential and privacy issues associated with student users that can directly be linked to passwords and the management of passwords (Kruger, Steyn, Medlin, & Drevin, 2008).

This study can also serve to prepare the students to be more security conscious when they enter the workforce full-time. Werner (2005) said that as employees, new college graduates will have access to critical data to perform their jobs yet they could be the weakest link in a secure computer system primarily because of inadequate education, negligence, and inexperience. The instruction and training as part of this study can not only meet the current demands of securing systems but also better prepare students for future employment in their respective fields.

Instruction and training

Because relatively few users have chosen to use password management applications, it was necessary in this study to first provide instruction and training to the student participants. Students needed an entire instructional “process” in order to understand password security and to have hands-on experience using a password management application. Only then would students be in a position to provide a reasoned response regarding their experiences and perceptions.

All student participants were required to complete a four-step process regarding password security and password management applications. First, the students read a 37-page chapter of material that included a running vignette, examples, figures, summary, and list of key terms regarding personal security and password management. Second, the students watched a 45-minute video of the chapter material. Third, the students took a 20-question assessment to determine their level of understanding of the material. Only after these steps were completed to provide the necessary foundation, the students then followed instructions how to download, install, and use a specific password management application. Once this activity was completed the students related on a survey their experiences, how likely they were to use the application, and the reasons for their decisions.

The depth of the training was considered to be an important element in this study. First, the broader background of password security was introduced to students, so they could have a context in which to understand password management applications. Second, by assessing student learning it served to validate student learning of the objectives. Third, by using different pedagogical approaches--auditory (lecture video), visual (textbook), and kinesthetic (hands-on use)—it met the needs of the different types of learners.

4. PILOT STUDY

A pilot study was first conducted prior to the actual study. A group of 21 participants read the material and viewed the lecture video. Upon completion of the video they were given a 20-question assessment (N=20, M=19, SD=0.92). Following the assessment the participants downloaded KeePass, an open source password management application, and installed it. They then were instructed to use the application to record a personal password and retrieve it for use.

The participants next were asked their opinions regarding the application in four key areas: 1) Is this an application that would help users create and use strong passwords?; 2) What are the strengths of these password programs?; 3) What are the weaknesses?; and 4) Would you use KeePass? Participant responses were open-ended narratives.

Of the 21 participants two indicated that they would use KeePass. Two additional participants indicated that they “might” or would “strongly consider” using the application. Ten participants stated that they would not use KeePass or a similar application. Their comments generally focused on three reasons: 1) no personal need for a password management application; 2) password management applications were inconvenient; and 3) the risk of an attacker stealing their master password and then having accessing to all stored passwords. Of the remaining seven participants, four provided comments but did not indicate if they would use the application personally. Three participants gave no comments.

5. STUDY

The study was conducted at a regional university and a community college. Student participants were from one of four sections of computer courses.

Of the 101 students who participated, 68 (67%) attended the university, of which 54 were male and 14 were female, while 33 (33%) students attended the community college (10 male and 23 female). A total of 61 students (60%) were employed (54 university students and 7 community college students).

All participants were required to complete a four-step process: 1) read a chapter of material regarding personal security and password management, 2) watch a lecture video, 3) take an assessment, and 4) download, install, and use the KeePass password management application. Once this activity was completed the students completed a survey regarding their experiences, how likely they were to use the application, and the reasons for their decisions.

6. RESULTS

Upon completion of reading the chapter of material regarding personal security and password management followed by viewing the video, all students were given a 20-question assessment regarding the material (N=101, M=16.67, SD=2.84). The purpose of the assessment was to both provide evidence that the students had actively engaged in reading and viewing the material and also to provide a message to the students about what they should be learning (Knight, 1995).

In order to examine student attitudes towards a password management application, four sets of survey questions were provided. These questions queried the students regarding the ease of use, benefits, and usefulness of the application.

Participant Attitudes Towards KeePass

The first set of questions was measured using a 5-point Likert scale, ranging from “1-Strongly Agree” to “5-Strongly Disagree”. The analysis of the results investigated the median, mean, and standard deviation of the attitude of the students towards their experiences using the KeePass password management program. These statistical results are listed in Table 1 and the median values are illustrated in Figure 1, both of which are found in the Appendix.

The results from Table 1 indicate that participants found KeePass easy to use (Question 1, Mdn=1, M=1.90, SD=1.29). They also recognized the strengths of a password management program: it can facilitate creating unique passwords (Question 2, Mdn=1, M=1.91, SD=1.23) and strong passwords (Question 4, Mdn=2, M=2.04, SD=1.29) that can be easily organized (Question 3, Mdn=2, M=1.93, SD=1.25). This can be done without resorting to using less secure methods of recording passwords (Question 6, Mdn=2, M=2.16, SD=1.42) or relying solely on memory (Question 7, Mdn=2, M=2.18, SD=1.37) and running the risk of forgetting passwords (Question 8, Mdn=2, M=2.25, SD=1.33). Students were not discouraged from using KeePass because it required its own password to be memorized (Question 12, Mdn=4, M=3.86, SD=1.34).

These results also indicate that students were able to identify the weaknesses of a password management program. These weaknesses include: losing the master password would result in a loss of access to all passwords (Question 10, Mdn=3, M=2.75, SD=1.16), an attacker who uncovers the master password would have access to all passwords (Question 5, Mdn=2, M=2.15, 1.20), and the application and user data must be carried with the user to other computers (Question 11, Mdn=3, M=3.18, 1.33). However, the primary advantage of a password management program--increasing security--did not receive as strong a participant response (Question 9, Mdn=2, M=2.36, SD=1.29) as may be expected.

Reasons for Using KeePass

Participants were also asked to respond why they would choose to use KeePass. A list of five options was given, and participants could select all that applied to them. Table 2 illustrates reasons why participants would choose to use KeePass.

Table 2. Reasons Participants Would Use KeePass

Question	Percentage
13. I do not have to memorize multiple passwords	76.2%
14. It's easy to use	75.2%
15. I do not have to write down my passwords on paper	55.4%
16. Using KeePass makes my account safer	51.5%
17. None of the above	3.0%

Students again identified the advantages of password management programs (Question 13 and Question 15) along with KeePass' ease of use (Question 14). When the responses of Table 2 were cross tabulated by employment there was little difference for Questions 13, 14, and 16 (the largest difference between employed and unemployed students for these three questions was only 2.5%). Question 15 accounted for the largest difference, with 50.8% (31 of 61) of those employed who said that they would use KeePass because they would not have to write down their passwords, while 62.5% (25 of 40) of those not employed said that this was a reason why they would use it. When these responses were cross tabulated by gender, 25 out of 37 females (67.6%) responded that KeePass enabled them to not have to write down their passwords (Question 15) while only 31 out of 64 males (48.4%) gave this as a reason why they would use it.

Once again students did not rate using KeePass as an activity that made their accounts safer (Question 16). A cross tabulation indicates that only 46.9% of males (30 of 64) said that KeePass made their accounts safer, while 59.5% of females (22 of 37) said it made their accounts safer. In addition, 42.4% of community college students (14 of 33) said that that KeePass made their accounts safer, compared to 55.9% (38 of 68) of university students.

Reasons for Not Using KeePass

Students were also asked to respond why they would not use KeePass. A list of eight options were given, and they could select all that they felt applied to them. Table 3 illustrates reasons why students would not choose to use KeePass.

The reasons listed in Table 3 indicate that students were aware of the weaknesses of password management programs, most notably that the loss of the KeePass password to an attacker would compromise all passwords (Question 18), that KeePass' usage is limited to only computers that have access to the program and the user's data (Question 21), and that forgetting the KeePass password would restrict access to all user passwords (Question 23). Question 19 may reveal an inconvenience—the KeePass application must first be launched when a password is needed—that students considered too burdensome.

Table 3. Reasons Participants Would Not Use KeePass

Question	Percentage
18. Someone could access all of my passwords if they uncover my KeePass password	66.3%
19. It is quicker for me to type in my passwords than to open KeePass to look up my passwords	56.4%
20. I already have all of my passwords memorized	53.5%
21. I can use any computer to access my account instead of only using a computer that has access to my KeePass information	45.5%
22. I am good at memorizing passwords	35.6%
23. I am afraid I will forget the KeePass password	28.7%
24. I already use strong passwords	27.7%
25. None of the above	5.9%

Questions 20 and 22 indicate that students feel comfortable relying on their memory for password retrieval. Students were also asked to self-report the number of computer accounts they used that required a password. The number of passwords reported (N=101, M=11.58, SD=10.00) is similar with other research on the number of user passwords. The range of passwords reported was from 59 to 1.

When the responses of Table 3 were cross tabulated by school, gender, and employment status it revealed several interesting findings. Employment seemed to play a factor in student responses. In Question 20 those students not employed said that they would not use KeePass, because they already had all of their passwords memorized (70%, 28 of 40) compared to those who were employed (42.6%, 26 of 61). In addition, employed students (14 of 61) were less likely to not use KeePass because they were good at memorizing passwords (Question 22) compared to those who were not employed (22 of 40), or 23.0% vs. 55.0%. In addition, employed students were less likely (37.7%, or 23 of 61) to not use KeePass, because they were restricted to using a computer that had KeePass or their data accessible (Question 21) compared to those who were not employed (57.5%, or 23 of 40).

Students attending a community college indicated that they have much better memories (Question 22) than those attending a university (45.5% or 15 of 33 vs. 30.9% or 21 of 68), yet they do not use strong passwords (5 of 33 or 15.2%) compared to students attending a university (23 of 68 or 33.8%), as seen in Question 24.

Males also said (Question 24) they already use a strong password (21 of 64 or 32.8%) compared to females (7 of 37 or 18.9%). Yet males are more fearful of forgetting the KeePass password (34.4%, 22 of 64) than females (18.9%, 7 of 37).

Future Plans for Using KeePass

Table 4 illustrates the student's responses regarding their future plans for using KeePass. Almost 3 in 10 participants either will use or already use a password management program, while 5 in 10 remain undecided. The remaining 2 in 10 will not use the program.

The cross tabulation analysis of Table 4 reveals that there is very little difference between genders regarding if they will, will not, or have not decided to use KeePass. For those students who are employed, there also is little difference between not using Keepass or being undecided. However, there was a larger difference between those employed who said that they would use KeePass (31.1%, 19 of 61) compared to those not employed (20.0%, 8 of 40).

A larger difference is seen between students based on the school that they attended. The larger number of students attending a university (30.9%, 21 of 68) said they would use KeePass, compared to only 18.2% (6 of 33) of those attending a community college. Also, participants at a community college (60.6%, 20 of 33) were more undecided than those attending a university (45.6%, or 31 of 68).

Table 4. Participant's Plans for Using KeePass

Question	Percentage
I have not decided	50.5%
Yes	26.7%
No	19.8%
I already use KeePass or a similar program	3.0%

6. DISCUSSION

Prior research had indicated that relatively few users have chosen to use password management applications to create strong passwords and protect them. The study by Gaw and Felten (2006) of 49 users who were told to bring "anything you use to help you remember your passwords" revealed that only six participants brought aids, none of which was a password management application. This led Gaw and Felten to conclude that these applications were "relatively unpopular".

For this study only 3% of the student participants already used a password management application, supporting the conclusion of Gaw and Felten. Were they "relatively unpopular" because users had rejected them as being unsuitable, or because users lacked prior exposure to these applications? The results of this study seem to indicate that once users receive instruction and training regarding password management applications followed by actual use of the application, the benefits become apparent. More students indicated that they would use a password management application like KeePass (26.7%) than those who said they would not (19.8%), and half of the students (50.5%) were unsure of which action they would take. This leads to the conclusion that the reason for the small number of users of password management application is not because they have tried the application and found it to be unsuitable; instead, they simply were not familiar with the application.

The results of this study indicating that once users receive instruction and training in a security application the benefits become apparent may have broader implications for security awareness instruction and user training, particularly in higher education. Training is emphasized by many researchers, including Long (1999), Tobin and Ware (2005), Werner (2005), Witson (2003), Yang (2001) and others. Although Long (1999) advocated that security instruction should begin as early as kindergarten, most researchers state that higher education should be responsible for providing security awareness instruction, including Crowley (2003), Mangus (2002), Null (2004), Tobin and Ware (2005), Valentine (2005), Werner (2005), and Yang (2001). This instruction and training is important not only to meet the current demands of securing systems but also to prepare students for employment in their respective fields, according to Werner (2005). Long (1999) maintained that the need for organizations to develop appropriate policies requires all decision makers to have a certain level of awareness of standards for security.

One area of additional study is to examine in greater detail the responses towards security technology as it relates to gender, type of school, and employment, as well as other factors. For example, in this study 70% of unemployed students said that they would not use KeePass because they already had all of their passwords memorized, compared to only 42.6% of those employed. In addition, only 23% of employed students said that they would not use KeePass because they were good at memorizing passwords compared to 55% of those unemployed who said they were good at memorizing passwords. Additional research may reveal if there is security training instruction at workplaces that are having a positive impact on user attitudes and practices towards security.

A final area for additional study may be alternative password management applications, particularly those that are not restricted to a local computer. In both the survey data as well as student responses the need to carry both the password management application and user data with them at all times in order to have access to passwords was a barrier to acceptance. Future research may look at other types of password management applications that do not have this limitation in order to determine if these applications are more appealing to users.

7. CONCLUSION

The results of this study seem to indicate that once users receive instruction and training regarding password management applications followed by actual use of the application, the benefits of managing multiple strong passwords may become apparent. This leads to the conclusion that the reason for the small number of users of password management application is not because they have tried the application and found it to be unsuitable; instead, they simply were not familiar with the application. This may have broader implications for security awareness instruction and user training, particularly in higher education.

8. REFERENCES

Brown, A., Bracken, E., Zolccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology , 18* (6), 641-651.

Bunnel, J., Podd, J., Henderson, R., Napier, R., & Kennedy-Moffat, J. (1997). Cognitive, associative and conventional passwords: Recall and guessing rates. *Computers and Security , 16* (7), 641-657.

Burnett, M., & Kleinman, D. (2006). *Perfect passwords: selection, protection, authentication.* Burlington, MA: Syngress.

Charoen, D., Raman, M., & Olfamn, L. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice and Action Research , 21* (1), 55-72.

Crowley, E. (2003). Information systems security curricular development. *Conference on Information Technology Education* (pp. 249-255). Lafayette, IN: ACM.

Dhamija, R., & Perrig, A. (2000). Deja vu: A user study using images for authentication. *Proceedings of the 9th USENIX Security Symposium.* Denver, CO.: USENIX.

Frincke, D., & Bishop, M. (2004). Joining the security education community. *IEEE Security and Privacy , 2* (5), 61-63.

Gaw, S., & Felten, E. (2006). Password management strategies for online accounts. *Symposium on Usable Privacy and Security* (pp. 44-55). Pittsburgh, PA: Association for Computing Machinery.

Goldberg, J., Hagman, J., & Sazawal, V. (2002). Doodling our way to better authentication. *Proceedings of Ext. Abstracts CHI 2002* (pp. 868-869). New York, NY: ACM Press.

Govindarajulu, N., & Madhvanath, S. (2007). Password management using doodles. *ICMI'07* (pp. 236-239). Nagoya, Aichi, Japan: ACM.

Knight, P. (1995). *Assessment for Learning in Higher education.* London: Kogan Page.

Kruger, H., Steyn, T., Medlin, B., & Drevin, L. (2008). An empirical assessment of factors impeding effective password management. *Journal of Information Privacy and Security , 4* (4), 45-59.

Long, C. L. (1999). A socio-technical perspective on information security knowledge and attitudes. *Ph.D. dissertation, The University of Texas at Austin, United States-- Texas* .

Mangus, T. (2002). A study of first-year community college students and proposed responsible computing guide. *Ph.D. dissertation, Union Institute and University, United States--Ohio* .

Miller, G. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychology Review , 63*, 81-97.

Neath, I. (1998). *Human memory: An introduction to research, data, and theory.* Pacific Grove, CA: Brooks/Cole.

Null, L. (2004). Integrating security across a computer science curriculum. *Journal of Competing Science is in Colleges , 19* (5), 170-178.

Pastore, M., & Dulaney, E. (2006). *CompTIA Security+ Study Guide* (3ed ed.). Indianapolis: Wiley.

Reichl, D. (2010). *KeePass features*. Retrieved Jan 16, 2010, from keepass.info: http://keepass.info/features.html

Sasse, M., & Brostoff, S. W. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. *BT Technology Journal , 19* (3), 122-131.

Schneier, B. (2004). *Secrets and lies: Digital security in a networked world.* New York: Wiley Computer Publishing.

Tari, F., Ozok, A., & Holden, S. (2006). Password management, mnemonics, and mother's maiden names: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. *Second Symposium on Usable Privacy and Security (SOUPS).* New York, NY: ACM Press.

Tobin, D., & Ware, M. (2005). Using a windows attack intRusion emulator (AWARE) to teach computer security awareness. *10th Annual SIGSCE Conference on Innovation and Technology in Computer Signs Education* (pp. 213-217). Caparica, Portugal: SIGSCE.

Topkara, U., Atallah, M., & Topkara, M. (2007). Passwords decay, words endure: Secure and re-usable multiple password mnemonics. *Proceedings of the 2007 ACM symposium on Applied computing* (pp. 292-299). Seoul, Korea: ACM.

Valentine, D. W. (2005). Practical computer security: A new service course based upon the national strategy to secure cyberspace. *Conference on Information Technology Education* (pp. 185-189). Newark, NJ: ACM.

Vu, K.-P., Proctor, R., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies* (65), 744-757.

Werner, L. (2005). Redefining computer literacy in the age of ubiquitous computing. *Conference on Information Technology Education* (pp. 95-99). Newark, NJ: ACM.

Whitson, G. (2003). Computer security: Theory, process and management. *Journal of computing sciences in colleges , 18* (6), 57-66.

Wiedenbeck, J., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. *SOUPS '05: Proceedings of the 2005 Symposium on Usable Privacy and Security* (pp. 25-31). New York: ACM Press.

Yan, J., Blackwell, A., Anderson, R., & GRant, A. (2004). Password memorability and security: Empirical results. *IEEE Security and Privacy , 2* (5), 25-31.

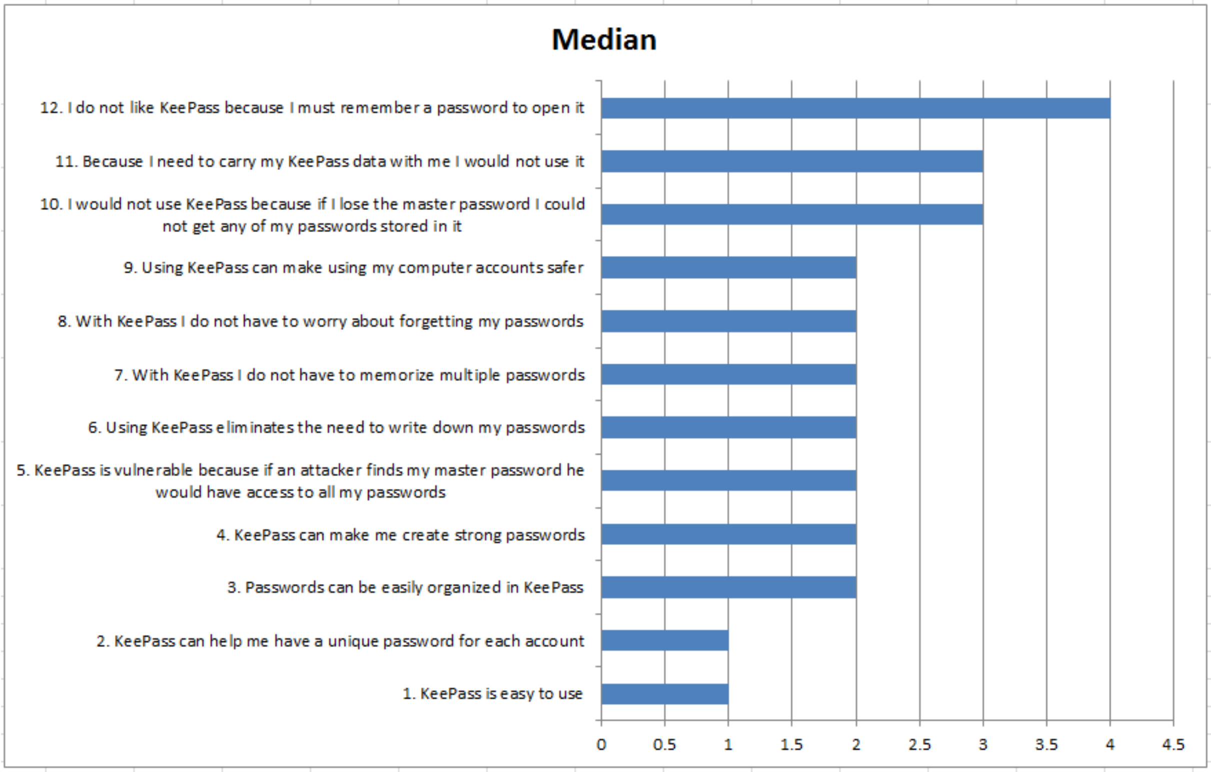
Yang, T. A. (2001). Computer security an impact on computer science education. *Journal of Computing Sciences in Colleges , 18* (6), 233-246.

Appendix

Table 1. Participant Attitudes with KeePass

Question	Median	Mean	Std Dev
1. KeePass is easy to use	1	1.90	1.29
2. KeePass can help me have a unique password for each account	1	1.91	1.23
3. Passwords can be easily organized in KeePass	2	1.93	1.25
4. KeePass can make me create strong passwords	2	2.04	1.29
5. KeePass is vulnerable because if an attacker finds my master password he would have access to all my passwords	2	2.15	1.20
6. Using KeePass eliminates the need to write down my passwords	2	2.16	1.42
7. With KeePass I do not have to memorize multiple passwords	2	2.18	1.37
8. With KeePass I do not have to worry about forgetting my passwords	2	2.25	1.33
9. Using KeePass can make using my computer accounts safer	2	2.36	1.29
10. I would not use KeePass because if I lose the master password I could not get any of my passwords stored in it	3	2.75	1.16
11. Because I need to carry my KeePass data with me I would not use it	3	3.18	1.33
12. I do not like KeePass because I must remember a password to open it	4	3.86	1.34

Figure 1. Median Participant Attitudes with KeePass


Median
12. I do not like KeePass because I must remember a password to open it
11. Because I need to carry my KeePass data with me I would not use it
10. I would not use KeePass because if I lose the master password I could not get any of my passwords stored in it
9. Using KeePass can make using my computer accounts safer
8. With KeePass I do not have to worry about forgetting my passwords
7. With KeePass I do not have to memorize multiple passwords
6. Using KeePass eliminates the need to write down my passwords
5. KeePass is vulnerable because if an attacker finds my master password he would have access to all my passwords
4. KeePass can make me create strong passwords
3. Passwords can be easily organized in KeePass
2. KeePass can help me have a unique password for each account
1. KeePass is easy to use