Journal of Applied Security Research
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/wasr20

Online Versus Local Password Management Applications: An Analysis of User Training and Reactions

Mark Ciampa [a], Mark Revels [a] & John Enamait [b]

[a] Information Systems, Western Kentucky University, Bowling Green, Kentucky, USA

[b] Dean of School of Business, Industry, and Technology, Catawba Valley Community College, Hickory, North Carolina, USA

Published online: 05 Oct 2011.

To cite this article: Mark Ciampa , Mark Revels & John Enamait (2011) Online Versus Local Password Management Applications: An Analysis of User Training and Reactions, Journal of Applied Security Research, 6:4, 449-466, DOI: 10.1080/19361610.2011.604070

To link to this article: http://dx.doi.org/10.1080/19361610.2011.604070

Journal of Applied Security Research, 6:449–466, 2011

ISSN: 1936-1610 print / 1936-1629 online
DOI: 10.1080/19361610.2011.604070

Routledge
Taylor & Francis Group

Online Versus Local Password Management Applications: An Analysis of User Training and Reactions

MARK CIAMPA
Information Systems, Western Kentucky University, Bowling Green, Kentucky, USA
MARK REVELS
Information Systems, Western Kentucky University, Bowling Green, Kentucky, USA
JOHN ENAMAIT
Dean of School of Business, Industry, and Technology, Catawba Valley Community College, Hickory, North Carolina, USA

This study compared a password management application using browser extensions with remote storage against a locallystored password management application. All participants were required to complete a 4-step training process culminating with the use of a password management application and a survey of their experiences. The mean responses from the survey questions were analyzed using an independent (unpaired) t*test of samples with unequal sizes assuming equal variance. The results indicate that once users receive instruction and training the benefits of managing multiple strong passwords using technology becomes apparent. Online storage password management applications may be more popular for users over locallystored applications.*

KEYWORDS Password, training, KeePass, LastPass

DEFINITIONS

The process of providing proof that a user is genuine and is not an imposter is known as authentication (Pastore & Dulaney, 2006). Authentication systems are based on the use of a physical token (whatonehas), a physical characteristic (whatone is), or secret knowledge (whatone knows) that can

Address correspondence to Mark Ciampa, 1906 College Heights Boulevard, Bowling Green, KY 42101, USA. E-mail: mark.ciampa@wku.edu

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) saidthat "systems are only as secure as the weakest password" (p. 139).

There are a variety of attacks that can be used to discover a password:

- Social engineering. Passwords can be revealed through social engineering attacks, including phishing, shoulder surfing, and dumpster diving.
- Capturing. There are several methods that can be used to capture passwords. A software or hardware keylogger on a computer can capture the passwords that are entered on the keyboard. While passwords are in transit, man-in-the-middle and replay attacks can also be used.
- Resetting. If an attacker can gain physical access to a user's computer, then the attackercan erase the existing password and reset it to a new one. Password reset programs require that the computer to be rebooted from a CD or USB flash drive that usually contains a version of a different operating system along with the password reset program.
- Online guessing. Although it is possible for an attacker to enter different passwords at the login prompt to attempt to guess a password, in reality this is not practical. An eight-character password that can use any of 76 characters of uppercase and lowercase letters, digits, and common symbols (character set) would result in 1.11×10^{15} possible passwords. At two or three tries per second, it could take 5,878,324 years to guess the right password. In addition, most accounts can be set to disable all logins after a limited number of incorrect attempts (such as five), thus locking out the attacker.
- Offline cracking. Given the limitations of online guessing, most password attacks today use offline cracking. Passwords are usually stored in encrypted form on a computer so that when a user enters their password to log on, that password is encrypted in the same way and compared with the stored encrypted version. If it matches the stored password, the user is approved. Attackers can steal the file of encrypted passwords and then load that file onto their own computer and can then attempt to discover the passwords by comparing the encrypted passwords with encrypted passwords that they have created. Once a match of encrypted passwords occurs, then the password is known.

There are several different offline cracking techniques. One is an automated brute force attack, in which every possible combination of letters, numbers, and characters is used to create encrypted passwords that are matched with those in the stolen file. Another is a dictionary attack. A

dictionary attack begins with the attacker creating encrypted versions of common dictionary words and then comparing them against those in a stolen password file. This can be successful because users often create passwords that are simple dictionary words. A hybrid attack will slightly alter dictionary words by adding numbers to the end of the password, spelling words backward, slightly misspelling words, or including special characters such as @, $, !, or %. Although brute force and dictionary attacks were once the primary tools used by attackers to crack an encrypted password, today attackers usually prefer rainbow tables. Rainbow tables make password attacks easier by creating a large pregenerated data set of encrypted passwords.

Password attacks are successful due to four significant weaknesses in passwords and their management. The first weakness 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 because 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).

The second weakness is the number of different accounts and passwords that are required today also places a load on a user's memory. In general, users have multiple accounts for different computers at work, school, and home, for various e-mail accounts, for online banking and Internet sites, just to name a few, and each account has its own password. Despite research by Gaw and Felten (2006) 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 and colleagues (2007) indicated that 35% of users had 3 to 4 passwords, 18% had 5 to 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 more than13 passwords each. Sasse and Brostoff (2001) reported that a group of 144 users had an average of 16 passwords per user, whereas Brown, Bracken, Zolccoli, and Douglas (2004) reported a group of college students ($N = 218$) averaged 8.18 passwords each. Choren and colleagues (2008) noted that because users have multiple accounts requiring multiple passwords, it is "more than slightly impossible" (p. 70) for users to remember each password.

The third weakness is the security policies that are created and enforced by the organization to ensure strong user passwords. These policies include "enforce password history" (the number of unique new passwords a user must use before an old password can be reused), "maximum password age" (how many days a password can be used before the user is required to change it), "minimum password length," "passwords must meet

complexity requirements," "account lockout duration" (the length of time a locked account remains unavailable before a user can try to log on again), and "account lockout threshold" (the number of failed log in attempts before a lockout occurs). Although well-intended, such policies often frustrate users and even encourage them to seek ways to circumvent the restrictions.

The final weakness is a lack of understanding by users regarding how a password attack program attempts to break a password. Most passwords consist of a root (not necessarily a dictionary word but generally pronounceable) along with an attachment, either an ending suffix (about 90% of the time) or a prefix (10%). An attack program will first test the password against 1,000 common passwords (such as 123456, password1, and letmein). If it is not successful, it then combines these common passwords with 100 common suffixes (such as 1, 4u, and abc). This results in almost 100,000 different combinations that can crack 25% of all passwords. Next the program (in order) uses 5,000 common dictionary words, 10,000 names, 100,000 comprehensive dictionary words, and combinations from a phonetic pattern dictionary, varying the dictionary words between lowercase (the most common), initial uppercase (the second most common), all uppercase, and then final character as uppercase. The program also makes common substitutions with letters in the dictionary words, such as $ for s, @ for a, 3 for E, and so forth. Last, it uses a variation of attachments, such as two-digit combinations, dates from 1900 to the present, three-digit combinations, single symbols (#, $, %), single digit plus single symbol, and two-symbol combinations (Schneier, 2007). Without this understanding of how password attack programs function, users typically create passwords that can easily be broken by these programs.

Because of these weaknesses, users typically create weak passwords. 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). In addition, users often 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 Fenten (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.

The problem with weak passwords can be illustrated through two recent security breaches. In December 2009, an attacker broke into a server using an SQL Injection Attack belonging to RockYou Inc., a developer of Facebook applications. This server contained more than 32 million user passwords that were all stored in an unencrypted format. The attacker later posted all 32 million passwords on the Internet. The database security vendor Imperva took the opportunity to analyze these real-world passwords to determine the types of passwords that users are creating today, as past studies only relied on user responses to surveys about their passwords. According to Imperva's analysis

of the length of these 32 million passwords, 30% of users created passwords whose length was only five (the Rockyou.com minimum length) or sixcharacters. Only 12% of the user passwords were ninecharacters in length. In terms of the character set, 60% of users chose their passwords from a limited set of characters, while another 16% used only digits, and fewer than 4% of the users used any special characters. Likewise, password complexity was weak. Almost 20% of the users used a password from a list of the 5,000 most popular passwords, which were names, slang words, dictionary words, or trivial passwords (e.g., consecutive digits, adjacent keyboard keys). The most common password among Rockyou.com account owners was "123456", found in 290,731 accounts (in second place was "12345"). Some of the other top 20 most frequently used passwords were "Password," "iloveyou," and "abc123" ("Data Security Study," 2009). In December 2010, attackers broke into Gawker Media's web servers and stole the authentication login credentials of more than1.3 million users as well as employee usernames and passwords. The security vendor Duo Security has analyzed this list of stolen passwords, and the five most common passwords that Gawker users created were (in order) "123456," "password," "12345678," "qwerty," "abc123," and "12345." Also, 99.45% of the cracked passwords used only an alphanumeric character set and did not contain any special characters or symbols (of these, 61% were only lowercase alphabetic characters and 9% were only numeric). Duo Security also revealed that 15 of the cracked accounts belonged to individuals working at the National Aeronautics and Space Administration, 9 were users who worked for Congress, and 6 belonged to employees of the Department of Homeland Security ("Brief analysis," 2010).

Schneier (2004) summarized the issue well by stating the following:

> 7 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 (p. 160).

Addressing Password Weaknesses

To overcome 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.

The first category comprisessolutions 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; the other is encoded in a mnemonic sentence (Topkara, Atallah, & Topkara, 2007).

The second category of solutions is substituting graphical passwords for the common textual passwords. Graphical passwords are based on the premise that figures or images are easier for users to recall than text and utilizing images are more difficult for an attacker to circumvent. 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), identifying a series of random art images (Dhamija & Perrig, 2000), requiring the user to identify specific faces (Tari, Ozok, & Holden, 2006). Even using personalized hand-drawn doodles for authentication has been proposed by several researchers (e.g., Goldberg, Hagman, & Sazawal, 2002; Govindarajulu & Madhvanath, 2007).

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.

The final category for addressing password weaknesses is to use technology. There are several different technologies that are available:

- Built-in browser function. Firefox and Internet Explorer contain a function to allow a user to save a password that has been entered while using the browser (called an *Auto Complete password* in Internet Explorer) or through a separate dialog box that pops up over the browser (called an *HTTP authentication password* in Internet Explorer). AutoComplete passwords are stored in the Microsoft Windows registry and are encrypted with a key created from the website address while HTTP authentication passwords are saved in the credentials file of Windows, together with other network login passwords. The disadvantage is that these passwords cannot be accessed when using another computer.
- Stand-alone password management application. Called by Gaw and Felten (2006) the "digital equivalent" (p. 50) to a written Post-It note, these programs let a user create and store multiple strong passwords in a single user file that is protected by one strong master password. This file is stored on the local computer or carried on a USB flash drive. Users can retrieve individual passwords as needed by opening the user file, thus freeing the user from the need to memorize multiple passwords. Examples are KeePass and Password Safe. The disadvantage is that users must carry the application

and protected file on USB flash drive or have it installed on each computer that is used.

- Browser extension with local storage. These browser extensions store the passwords locally. Examples are Password Multiplier, RoboForm, Auora, and Handy Password. The disadvantage is that users cannot access passwords from another computer.
- Browser extension with remote storage. Instead of storing the passwords locally, the passwords are stored online. Examples include RoboForm Online Beta and LastPass. The disadvantage is that each computer must have the browser extension installed.
- Browser extension that generates passwords. Instead of storing user-created passwords, these extensions transparently hashing multiple elements (e.g., the username, master password, and site's domain name) into a single site-specific password. The user begins by entering their username and master password, and then the extension generates their site-specific password. The remote site only sees a domain-specific hash instead of the master password itself. Examples include SuperGenPass, PwdHash, Lucent Personalized Web Assistant, and Passpet. The disadvantage is that they can only be used for Web-based passwords.
- Online password manager. These store all user passwords online. Examples include ClipperZ, Passpack, and Mitto. The disadvantage is that an attacker could attempt to break the online storage security.

Despite the advantages of using technology for password management, relatively few users have chosen to use them. In a study by Gaw and Fenten (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.)" (p. 46). Only six participants brought aids, none of which was a password management application. Gaw and Fenten (2006) concluded that these applications "interrupt the user's behavior" and were "relatively unpopular" (p. 471). However, they also stated that "technology solutions could help." Halderman, Waters, and Felten (2005) said,"Unfortunately, the inconvenience of available software has prompted many frustrated users to resort to [an] insecure strategy."

STUDY

This study compared a management application that utilized browser extensions (using remote storage) with a locallystored password management application. A previous study explored only the use of locallystored password management application (Ciampa, 2011). The goals were (a) to determine whetherremote storage password management applications are more

popular for users to implement over locallystored password management applications; (b) to determine the reason why password management applications were used so infrequently (was it because users were familiar with them and had rejected them as poor solutions, or was it because they were unaware of these applications and their benefits?); and (c) to determine if users be more inclined to use these applications once they received training about them.

The primary research hypothesis was as follows:

> Null hypothesis: No significant difference exists between user attitudes regarding the use of remote storage and a locallystored password management application.
>
> Hypothesis 1: Users demonstrate a preference of remote storage over a locallystored password management application.

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. (2008) noted that modern universities, with their core business focused on teaching and research, are managed and operated along the same line as is any business. In addition, there are a large number of confidential and privacy security issues associated with student users that can directly be linked to passwords and the management of passwords (Kruger et al., 2008).

The participants in this project were undergraduate student volunteers. Using these students as participants was important to the study. First, it allowed a comparison between the responses of those students who were employed and those who were not employed, which obviously would not be possible in a work environment where all individuals are employed. By evaluating the responses of employed students against those not employed this data could be used to determine whetheremployment and its associated training and security policies play a factor in a student's evaluation of password management applications. A second reason is many of these students are employed in staff positions instead of technical or managerial positions. Attackers frequently target these same staff employees because they represent a broad base of employees. Understanding the perceptions of a sample of these staff employees may help provide information for improved security processes for the larger population. Last, the study can help 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.

The study was conducted at a regional university and a community college. Student participants were from one of seven sections of computer courses. Of the 231 total participants, 71 (30%) attended a community college (27 male and 44 female), whereas 160 (70%) attended a university, of which 107 were male and 53 were female. A total of 137 participants (59%) were employed (114 from a university and 23 from a community college). The participants were divided into two groups, those who used a browser extension with remote password storage (131 used the LastPass application) and those who used a locallystored password management application (101 used KeePass).

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 participants. Participants needed an entire instructional process to understand password security in order to create a valid context and to have hands-on experience using a password management application. Only then would participants be in a position to provide a reasoned response regarding their experiences and perceptions. 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 participants so that they could have a context in which to understand password management applications. Second, by assessing participant learning it served to validate 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.

All participants were required to complete a four-step process regarding password security and password management applications. First, the participants 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, they watched a 45-min video of the chapter material. Third, the participants 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 participants then followed instructions how to download, install, and use a specific password management application (LastPass or KeePass). Once this activity was completed they related on a survey their experiences, how likely they were to use the application, and the reasons for their decisions.

Upon completion of reading the chapter of material regarding personal security and password management followed by viewing the video, all participants were given a 20-question assessment about the material that was read and viewed ($M = 17.29$, $SD = 0.19$). The purpose of the assessment was to provide feedback that the participants had actively engaged in

TABLE 1 Participant Attitudes

Question	t	sig	Results
1. LastPass/KeePass can make me create strong passwords	−3.96	0.000100	Reject Null
2. I do not like LastPass/KeePass because I must remember a password to open it	+0.34	0.734167	Accept Null
3. LastPass/KeePass is easy to use	−1.37	0.172023	Accept Null
4. Because of its limitation (must install LastPass on all of my computers/I need to carry my KeePass data with me) I would not use it	+1.61	0.108769	Accept Null
5. Passwords can be easily organized in LastPass/KeePass	−1.9	0.058684	Accept Null
6. LastPass/KeePass is vulnerable because if an attacker finds my master password he would have access to all my passwords	+1.14	0.255472	Accept Null
7. LastPass/KeePass can help me have a unique password for each account	−1.52	0.129884	Accept Null
8. I would not use LastPass/KeePass because if I lose the master password I could not get any of my passwords stored in it	+4.5	<.0001	Reject Null
9. Using LastPass/KeePass eliminates the need to write down my passwords	−1.4	0.162861	Accept Null
10. With LastPass/KeePass I do not have to worry about forgetting my passwords	−2.77	0.006063	Reject
11. With LastPass/KeePass I do not have to memorize multiple passwords	−2.84	0.004916	Reject Null
12. Using LastPass/KeePass can make using my computer accounts safer	−2.5	0.013117	Reject Null

reading and viewing the material and to provide a message to the participants about what they should be learning (Knight, 1995).

RESULTS

To examine participant attitudes towards a password management application four sets of survey questions were provided. The first set of questions was measured using a 5-point Likert-type scale, ranging from 1 (*strongly agree*) to 5 (*strongly disagree*), regarding the attitude of the participants towards their experiences using the LastPass or KeePass password management program.

The mean responses from the survey questions were analyzed using an independent (unpaired) *t*test of samples with unequal sizes assuming equal variance. The results are illustrated in Table 1. Note that the degrees of freedom are 231 for each question.

The results from Table 1 indicate that participants found a remote storage password management application (LastPass) would help them create strong passwords (Question 2), they would not use it due to the risk of losing

TABLE 2 Reasons Participants Would Use LastPass or KeePass

Question	LastPass	KeePass
13. It's easy to use	72.3%	75.2%
14. I do not have to memorize multiple passwords	68.5%	76.2%
15. Using LastPass/KeePass makes my account safer	39.2%	51.5%
16. I do not have to write down my passwords on paper	51.5%	55.4%
17. None of the above	4.6%	3.0%

the master password (Question 8), that it would help them not worry about forgetting passwords (Question 10), they would not have to memorize multiple passwords (Question 11), and it would make using computer accounts safer (Question 12) over a locallystored password management application (KeePass).

Participants were also asked to respond why they would choose to use LastPass or 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 the application.

Participants highly rated the advantages of password management programs (Question 14 and Question 16) along with the ease of use (Question 13). A cross-tabulation by employment for LastPass showed that there was little difference between Questions 13 and 14. However, only 32.9% of those employed said that using LastPass would make their accounts safer. For KeePass when the responses of Table 2 were cross tabulated by employment there was little difference for Questions 13, 14, and 15 (the largest difference between employed and unemployed participants for these three questions was only 2.5%). Question 16 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 women (67.6%) responded that KeePass enabled them to not have to write down their passwords (Question 16) while only 31 out of 64 men (48.4%) gave this as a reason why they would use it.

It is interesting to note that participants did not highly rate using LastPass or KeePass as an activity that made their accounts safer (Question 15). With LastPass 40.6% of men (28 of 69) said it would make their accounts safer and 38.3% of womenechoed that sentiment (23 of 60). Exactly half (19 of 38) of those attending a community college said that LastPass could make their accounts safer, compared with 35.1% of university participants (32 of 91). For KeePass a cross tabulation indicates that only 46.9% of men (30 of 64) said that KeePass made their accounts safer, while 59.5% of women (22 of 37) said it made their accounts safe. In addition, 42.4% of community

TABLE 3 Reasons Participants Would Not Use LastPass or KeePass

Question	LastPass	KeePass
18. I already have all of my passwords memorized	30.0%	53.5%
19. It is quicker for me to type in my passwords than to open LastPass/KeePass to look up my passwords	17.7%	56.4%
20. I already use strong passwords	22.3%	27.7%
21. I am good at memorizing passwords	19.2%	35.6%
22. I can use any computer to access my account instead of only using a computer that has access to my LastPass/KeePass information	29.2%	45.5%
23. I am afraid I will forget the LastPass/KeePass password	20.0%	28.7%
24. Someone could access all of my passwords if they uncover my LastPass/KeePass password	55.4%	66.3%
25. None of the above	20.8%	5.9%

college participants (14 of 33) said that that KeePass made their accounts safer, compared with 55.9% (38 of 68) of university participants.

Participants 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. Table 3 illustrates reasons why participants would not choose to use LastPass or KeePass.

The responses from Table 3 illustrate the differences between a remote storage (LastPass) over a locallystored password management application (KeePass). Whereas the LastPass application has the ability to automatically recognize the user's account information as it is being entered into the browser, KeePass requires that the application be launched and the information be dragged and dropped into the appropriate fields (this may also account for the differences in Question 19). In addition, the limitations of requiring that KeePass must be installed on each computer (or carried on a USB flash drive) may account for the higher percentage of users in Question 22 indicating they would not use it. Although the version of the LastPass application required that the browser extension must also be installed on each computer, users may have perceived that becausethe passwords themselves are stored remotely, they could be accessed more universally.

An interesting element is the high number of users who state that they already use strong passwords (Question 20). When broken down by application and gender, 23% of menusing LastPass and 21.7% of womensaid they used strong passwords. When examined by employment, the values were almost identical: 22.4% of those employed and 22.6% of those not employed claimed to use strong passwords. Men using KeePass said they already use a strong password (21 of 64 or 32.8%) when compared to females (7 of 37 or 18.9%).

Participants were also asked to self-report the number of computer accounts they used that required a password. The number of passwords

TABLE 4 Participant's Future Plans for Using LastPass or KeePass

Question	LastPass	KeePass
I have not decided	34.9%	50.5%
Yes	45.7%	26.7%
No	10.1%	19.8%
I already use a similar program	9.3%	3.0%

reported ($N = 228$, $M = 10.32$, $SD = 8.10$) is similar with other research on the number of user passwords. The range of passwords reported was from 59 to 1.

Table 4 illustrates the participant's responses regarding their future plans for using a password management application.

On the basis of the higher percentage of participants indicating that they plan to use LastPass over KeePass this may indicate that a remote storage password management applications may be more popular over locallystored password management applications. Open-ended comments from participants frequently focused on the inability to access KeePass from any computer without the software or user data. These included the following:

- "Another fault would be if you must memorize multiple passwords at work also, and you can't take this program with you."
- "Even though this program is 'portable' it seems like to me it would be more of a hassle than it is worth. What if I needed to log in to a website that had a highly encrypted password that I couldn't remember, and didn't have the flash drive with this software loaded with me?"
- "The con is that if you were not at a computer with KeePass access you couldn't access the accounts if you didn't know the password."

Other comments regarded the applications included the following:

- "Yes, this application can help other users create stronger passwords and not have to worry about memorizing the harder one and as long as they log in and out of the LastPass properly, they can protect their accounts"
- "I definitely think this is an excellent program because I forget my passwords all the time and have to call IT support to retrieve them"
- "Yes this application would help users to create and use strong passwords, since users do not have to remember their passwords, LastPass does it for you, and the user could create long complicated passwords that would be impossible to guess. That being said, if the user ever wanted to access their accounts on a computer that does not have LastPass, there would be no way for them to login."

DISCUSSION

The results of this study seem to indicate that remote storage password management applications may be more popular for users to implement over locallystored password management applications. The restrictions of having the application and the data file containing the passwords either installed on the computer or carried at all times on a USB flash drive, along with the need to open the application whenever a password must be retrieved, may pose to be too much of an inconvenience to average users. A browser-based extension with remote storage may prove to be more popular due to its advantages of automatically populating user account information from passwords stored online. The results from the study indicate that participants found a remote storage password management application would help them create strong passwords, that it would help them not worry about forgetting passwords, they would not have to memorize multiple passwords, and it would make using computer accounts safer over a locallystored password management application.

The results of this study also 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 becomes apparent. A small percentage of users (9.3% for LastPass and 3.0% for KeePass) already used a password management application, supporting the conclusion of Gaw and Fenten that these applications were "relatively unpopular." After receiving training and using the applications a higher percentage of participants indicated that they would use these applications than those who indicated they would not, although for KeePass the undecided users were still half of the total number of participants.

This 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 participants for employment in their respective fields. Werner 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 (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.

Support for making higher education the primary source for security awareness training comes from several different sources. The Action and Recommendation 3–4 of the National Strategy to Secure Cyberspace (NSSC) calls for colleges and universities to model user awareness programs and materials (Valentine, 2005). Frincke and Bishop (2004) summarized several of the major groups and efforts currently involved in computer security education with higher education institutions. These include the Colloquium for Information Systems Security Education, the International Federation of Information Processing Working Group 11.8 on Information Security Education, and the Workshop on Education in Computer Security. The National Security Agency also had developed an effort aimed at creating a larger core of computer security trained professionals known as the National Centers of Academic Excellence in Information Assurance Education, which even provides large numbers of college scholarships under its Cyber Corps Program.

The location of security awareness instruction and training in a college curriculum should not be isolated in upper-level courses for information technologymajors, according to Tobin and Ware (2005), Werner (2005), and others. This instruction should be taught to all graduates as a "security awareness" course (Valentine, 2005, p. 185) along with integrating it across through the curriculum (Yang, 2001).

One area of additional study is to examine in greater detail the responses towards security technology as it relates to gender, type of school, employment, as well as other factors. For example, in this study 70% of unemployed participants 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 participants 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 whetherthere is security training instruction at workplaces that has a positive effecton user attitudes and practices toward security.

Another area for study may be examining other alternative password management applications that provide even more ease-of-use for average users. This may help to identity applications that are most suitable for users.

CONCLUSION

The results of this study indicate that remote storage password management applications may be more popular for users to implement over locally-stored password management applications. In addition, 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 were not familiar with the application. This may have broader implications for security awareness instruction and user training, particularly in higher education. Instruction regarding security awareness in colleges and universities should be practical as well as available to all students.

REFERENCES

Brief analysis of the Gawker password dump. (2010, December 18). Retrieved from http://blog.duosecurity.com/2010/12/brief-analysis-of-the-gawker-password-dump

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

Ciampa, M. (2011, June). Are password management applications viable? An analysis of user training and reactions. *Information Systems Education Journal*, *9*, 4–13.

Crowley, E. (2003). Information systems security curricular development. *Conference on Information Technology Education* (pp. 249–255). Lafayette, IN: Association of Computing Machinery.

Data Security Study: Consumer Password Worst Practices. (2009, December). Retrieved from http://www.imperva.com/ld/password_report.asp

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. In L. Terveen (Ed.), *Proceedings of Extended Abstracts CHI 2002* (pp. 868–869). New York, NY: ACM Press.

Govindarajulu, N., & Madhvanath, S. (2007). Password management using doodles. *International Conference on Multimodal Interfaces'07* (pp. 236–239). Nagoya, Aichi, Japan: ACM.

Halderman, J., Waters, B., & Felten, E. (2005). A convenient method for securely managing passwords. *World Wide Web Conference* (pp. 10–19). Chiba, Japan: ACM.

Knight, P. (1995). *Assessment for learning in higher education*. London, England: 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.

Mangus, T. (2002). *A study of first-year community college students and proposed responsible computing guide*. Ph.D. dissertation, Union Institute and University, Cincinnati, 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 in Colleges*, *19*, 170–178.

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

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

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

Schneier, B. (2007, January 11). *Secure passwords keep you safer*. Retrieved from http://www.wired.com/politics/security/commentary/securitymatters/2007/01/72458?currentPage=all

Tari, F., Ozok, A., & Holden, S. (2006, July). *Password management, mnemonics, and mother's maiden names: A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords*. Paper presented at the 2nd Symposium on Usable Privacy and Security (SOUPS), New York, NY.

Tobin, D., & Ware, M. (2005, March). *Using a windows attack intRusion emulator (AWARE) to teach computer security awareness*. Paper presented at the 10th Annual SIGSCE Conference on Innovation and Technology in Computer Signs Education, Caparica, Portugal.

Topkara, U., Atallah, M., & Topkara, M. (2007). Passwords decay, words endure: Secure and re-usable multiple password mnemonics. In Y. W. Koo (Ed.), *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.

Wiedenbeck, J., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In L. F.

Canor (Ed.), *SOUPS '05: Proceedings of the 2005 Symposium on Usable Privacy and Security* (pp. 25–31). New York, NY: 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*, 233–246.

Yee, K. (2006, February 8). *How to manage passwords and prevent phishing*. Retrieved from http://usablesecurity.com/2006/02/08