18/11/2016

Dale Stubbs - 14024149

MANCHESTER METROPOLITAN UNIVERSITY

**Your PassWORD is Outdated**

*An Upgrade to PassSENTENCE is advised!*

*Literature Review*

Passwords have been used since ancient times. They were originally used in Ancient Rome and were called ‘watchwords’. It is explained that during the night watch in Roman times a wooden tablet with a watchword inscribed upon it is passed to each of the watchmen before they are relieved of their duties (Polybius. and Shuckburgh, 2012). Passwords have come a long way since the dawn of the computer. They were first used in computing systems in 1961 when the first Unix system had a login page in which a user entered their secret password in order to log onto the system (Crisman, P.A., 1965). Since this time passwords and their uses have evolved almost as much as computers themselves and have become an everyday essential for anyone with a computer.

Passwords are the most frequent (Kuo, C., Romanosky, S. and Cranor, L.F., 2006 and Chiasson, Oorschot and Biddle, 2006) and the most relied upon a form of authentication practised to date. They are used to protect any and all information that users have online that they believe to be important and therefore needs protecting. The passwords and usernames required for access to this information are similar to locking a piece of paper into a cabinet using a lock and key. As such an important feature of protecting this confidential information, the security of the passwords needs to be paramount.

With the security being so important thoughts suggest that the requirements when creating new account passwords would encourage the creation of complex passwords in order to maintain the safety of the contained information. This is not the case. Current systems support poor practice construction methods (Gaw, S. and Felten, E.W., 2006). This leads to the passwords being created becoming easy to guess and therefore their security becoming far from what it needs to be (Chiasson, Oorschot and Biddle, 2006). Creating a ‘not too easy to guess’ password if far from difficult as there are many websites that offer guidance for the creation of secure passwords. The difficulty becomes when a user needs to remember multiple different passwords and where each password is used. Developers have attempted to aid the user in remembering the password by giving the user the ability to enter a ‘password reminder’ text box when creating a new account. This can be useful at times but if the password has been forgotten then no amount of reminders will allow the user to remember.

The growth of e-commerce has increased the number of accounts that any one user may have (Ives, B., Walsh, K.R. and Schneider, H., 2004). In turn, this has increased the number of passwords required and has forced the user to remember more and more passwords. Some have found this difficult and have turned to password reuse (Ives, B., Walsh, K.R. and Schneider, H., 2004 and Gaw, S. and Felten, E.W., 2006). This concept has the benefit of distilling the number of passwords needing to be remembered down to only a few, however, the issue raised with this concept is that it is only as secure as the weakest system the passwords is being used on (Ives, B., Walsh, K.R. and Schneider, H., 2004). The failure to address and solve the issue of password reuse will only result in the problem becoming bigger and bigger as e-commerce continues to grow (Gaw, S. and Felten, E.W., 2006).

As technology advances, developers are looking into using biometrics as an alternative authentication system. On the face of it, this seems like the most logical path to take as fingerprints are unique to an individual as is their retinal scan. This could potentially eliminate an attacker’s ability to gain access to the users’ information and therefore ensuring its safety and confidentiality. This is not the case. ‘Gummi’ fingers that were made from the same ingredients that are found in gelatine sweets managed to fool fingerprint scanners 80% of the time (Matsumoto, 2002). Retinal scanners are a good form of authentication as a prosthetic eye with a matching retina could be very expensive and time-consuming to create, however, the drawback of this method is that whenever the scanner shines the light into the users’ eye they were left feeling ‘quite dazzled after multiple uses’ which is far from ideal (Hall, 2016). These forms of authentication come with their own set of disadvantages too. A list of which can be found in a paper by Chien Le in 2006 on the advantages and disadvantages of technologies (Le, C. 2006).

As passwords seem irreplaceable several attempts have been made to solve the issue of password reuse. Mark Keith, Benjamin Shao, Paul John Steinbart have written a paper on the use of passphrases for authentication (Keith, Shao and Steinbart, 2007). This mitigates the vulnerability to Dictionary Password attacks but does nothing for the user in terms of remembering a lot of phrases and where each of them has been used. The next attempt solve was the use of Mnemonic Phrase-based passwords. One particular example from a study conducted in 2006 was the phrase: ‘Four score and seven years ago, our Fathers’ from the Abraham Lincoln Gettysburg address being converted into the password ‘4s&7yaoF’. On the face of it, this would seem to be a perfectly legitimate, complex password to have, however, when an attacker builds a ‘dictionary’ to use for their password attack they would place substitutions into for certain words. For example, the words four, for and fore would all be replaced with the number 4 thus increasing the chances of the attacker eventually obtaining the correct password. Upon the conclusion of this experiment, it was shown that method was no more secure than using a regular phrase. When using a 400,000-word dictionary 4% of the mnemonic passwords were obtained in comparison to the 1.2 million word ‘standard’ dictionary used for cracking passwords obtaining 11% of the control passwords(Kuo, C., Romanosky, S. and Cranor, L.F., 2006).

The security of the web-based password managers seems increasingly easier to defeat. In four of the five tested managers, an attacker could steal arbitrary credentials of the user (Li, Z., He, W., Akhawe, D. and Song, D., 2014). Some web-based managers store the passwords locally on the users’ hard drives and in order to find these passwords developers have created a tool called Lupin. Lupin can explore passwords stored for 1,000 web pages in 35 seconds and 28% of the 45,000 most popular websites around to date are vulnerable to Lupin (Gonzalez, R., Chen, E.Y. and Jackson, C., 2013).

Another direction taken to solve the issue was the use of a Password Manager. This concept has various platforms available from stand-alone programs to web-based password managers. A password manager is a program that stores the users’ passwords and keeps them under the protection of the master password. This distills the users need to remember passwords down to a single one, the master password (Stobert and Biddle, 2014). Some passwords managers actually generate and store passwords for the user which eliminates the users’ problems even further as they would not even have to think of a password themselves. This turned out to be not as popular as predicted. People were not comfortable with the idea of handing over control of their passwords to a password manager (Chiasson, Oorschot and Biddle, 2006). Another flaw in this system was the single point of failure. A single password used to protect all other passwords meaning if the master password was acquired by an attacker, they would have access to all of the users’ passwords. Most importantly, the usability of the password managers needs to be as user-friendly as possible (Chiasson, Oorschot and Biddle, 2006).

A study by Stobert and Biddle in 2014 propose that we overcome the issues associated with passwords by developing a new type of password manager that does not store the passwords directly but uses different approaches to trigger the users’ memory of what the password for the account is. Their particular password manager had several issues and limitations including a lack of understanding of how it actually worked, security issues and incorrect interface elements (Stobert, E. and Biddle, R. 2014) concluding that there is a need to have a good balance between usability and security.

In 1999 a study was conducted by Alma Whitten and J. D. Tygar on the usability of a software called PGP 5.0 (Whitten, A. and Tygar, J.D., 1999). PGP is an encryption programme that is used to encrypt and decrypt data communications such as text, emails, files and folders. The programme is believed to have a ‘good’ user interface by ‘general standards’. They were able to define usability as:

Security software is usable if the people who are expected to use it:

1. Are reliably made aware of the security tasks they need to perform;

2. Are able to figure out how to successfully perform those tasks;

3. Don't make dangerous errors; and

4. Are sufficiently comfortable with the interface to continue using it.

The participants of this study were twelve people who were experienced users of email and had no previous knowledge of public and private key cryptography. Each participant was given the scenario that they were given the job of a political campaign coordinator and were required to send out updates of the campaign plan to the other members of the campaign team via email and using PGP 5.0 for privacy and authentication. The participants also had a 90-minute time limit in order to achieve this goal.

The experiment concluded with only one-third of the participants successfully signing and encrypting the email message within the 90 minutes time limit. Many of the participants showed unhappiness and frustration with the experience of using PGP 5.0 and confirmed that it was unlikely they would continue to use it in the real world. The conclusion of this experiment shows that the usability of any software is paramount to its success. If people find it easy to use then they will use it.

The book Security and Usability, written by Cranor and Garfinkel, states that “Increasingly, well-publicized security breaches are attributed to human errors that might have been prevented through more usable software.” (Cranor and Garfinkel, 2005). The book also suggests that in order for a password manager to be effective there needs to be a balance between the usability of the manager and the security that it provides. This is backed up by the findings of the study by Chiasson, Oorschot and Biddle.

This study was an examination to deduce if any progress had been made since the Whitten and Tygar experiment from 6 years earlier. Within their study, they examined the usability of two different password managers, PwdHash and Password Multiplier. Their study examined twenty-seven adults who were deemed to be ‘typical users of these systems’. All participants were given a list of instructions of how to use both of the managers. Each participant took part in a one-hour session in which they were required to complete five tasks that had been designed to simulate ‘real life’ uses of the managers. These tasks were to log in, migrate password, remote log in, update password and finally a second log in.

Upon completion of this study only one of the tasks set had a greater than 50% success rate (the second log in for PwDHash). Even after the instructions were given to them most of the participants still failed to complete more than half of the tasks. The conclusion drawn from this experiment was to add two additional criteria to the four points of defining a software as usable in the previous experiment. These are:

1. be able to tell when their task has been completed;

2. Have sufficient feedback to accurately determine the current state of the system.

The underlying message of this experiments conclusion is that that “Even the most technically secure system, if unusable, will fail in practice.” (Chiasson, Oorschot and Biddle, 2006).

In 2003 Deborah Abratt, Wayne Mallinson and Antonet Bekker wrote a paper on ‘Usability Testing: Recipe for Success’ for EuroStar (Abratt, D., Mallinson, W. and Bekker, A., 2003). In the paper, they compare multiple case studies and evaluated different aspects of each case including usability. The paper concludes that an increase in software usability testing, either with testers only or using testers and users, can offer significant benefits including user productivity.

After completing the analysis all of the papers within this literature review the main issue that has been highlighted is the usability of the software. If a piece of software has a complicated system of use then it is less likely that a user will use the software on a daily basis. Any future attempts to solve the issue of password reuse will need to address the issue of usability as the most important feature. It would also need to address any security shortcomings of its preceding competitors. There needs to be a good balance between usability and security tied into the new software.

# References

Polybius and Shuckburgh, E. (2012). The Histories of Polybius. 1st ed. Cambridge: Cambridge University Press.

Crisman, P.A. ed., (1965). The compatible time-sharing system: A programmer's guide. Mit Press.

Chiasson, S., Oorschot, P. and Biddle, R. (2006). A Usability Study and Critique of Two Password Managers. In Usenix Security (Vol. 6). Available at: https://www.usenix.org/legacy/events/sec06/tech/full\_papers/chiasson/chiasson.pdf [Accessed 11 Nov. 2016].

Gonzalez, R., Chen, E.Y. and Jackson, C., (2013). Automated password extraction attack on modern password managers. arXiv preprint arXiv:1309.1416.

Kuo, C., Romanosky, S. and Cranor, L.F., (2006). Human selection of mnemonic phrase-based passwords. In Proceedings of the second symposium on Usable privacy and security (pp. 67-78). ACM.

Ives, B., Walsh, K.R. and Schneider, H., (2004). The domino effect of password reuse. Communications of the ACM, 47(4), pp.75-78.

Gaw, S. and Felten, E.W., (2006). Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and security (pp. 44-55). ACM.

Li, Z., He, W., Akhawe, D. and Song, D., (2014). The emperor’s new password manager: Security analysis of web-based password managers. In 23rd USENIX Security Symposium (USENIX Security 14) (pp. 465-479).

Matsumoto, T. (2002). *Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies---A Case Study for User Identification---*. 14th ed. [ebook] Seoul. Available at:http://perso.telecom-paristech.fr/~chollet/Biblio/Articles/Domaines/BIOMET/spoof-fp5p4.pdf [Accessed 11 Nov. 2016].

Hall, C. (2016). *Microsoft Lumia 950 review: The dawn of Windows 10 Mobile - Pocket-lint*. [online] Pocket-lint.com. Available at: http://www.pocket-lint.com/review/136018-microsoft-lumia-950-review-the-dawn-of-windows-10-mobile [Accessed 11 Nov. 2016].

Cranor, L. and Garfinkel, S. (2005). Security and usability. 1st ed. Beijing: O'Reilly.

Adams, A. and Sasse, M. (1999). USERS ARE NOT THE ENEMY. COMMUNICATIONS OF THE ACM, [online] (Volume 42 Issue 12), pp.40-46. Available at: http://cacm.acm.org.ezproxy.mmu.ac.uk/magazines/1999/12/7773-users-are-not-the-enemy/fulltext [Accessed 18 Nov. 2016].

Whitten, A. and Tygar, J.D., (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security (Vol. 1999).

Abratt, D., Mallinson, W. and Bekker, A., (2003). Usability Testing: Recipe for Success. STARWEST: International Conference on Software Testing Analysis and Review.

Le, C. (2006). A Survey of Biometrics Security Systems [online]. Available at: http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/index.html [Accessed 18 Nov. 2016].

Keith, M., Shao, B. and Steinbart, P. (2007). The usability of passphrases for authentication: An empirical field study. International Journal of Human-Computer Studies, [online] 65(1), pp.17-28. Available at: http://www.sciencedirect.com.ezproxy.mmu.ac.uk/science/article/pii/S1071581906001236 [Accessed 18 Nov. 2016].

Stobert, E. and Biddle, R. (2014). A Password Manager that Doesn’t Remember Passwords. [online] pp.39-52. Available at: http://delivery.acm.org.ezproxy.mmu.ac.uk/10.1145/2690000/2683471/p39-stobert.pdf?ip=149.170.3.14&id=2683471&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2E8670C7C518068584%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=694905259&CFTOKEN=42396938&\_\_acm\_\_=1479486129\_0cf6d461849a9a6386a636d68c65f51e [Accessed 18 Nov. 2016].