Winter 12-13-2015

Social media is weakening passwords

Joseph Buckman
University of Arizona

Justin Giboney
University at Albany, SUNY

Yuan Hong
University at Albany, SUNY

Social media is weakening passwords

Research in progress

Joseph Russell Buckman
University of Arizona, Tucson, Arizona, USA {jbuckman@email.arizona.edu}

Justin Scott Giboney
University at Albany, SUNY, Albany, New York, USA {jgiboney@albany.edu}

Yuan Hong
University at Albany, SUNY, Albany, New York, USA {hong@albany.edu}

ABSTRACT

Passwords are often generated from readily available information such as family names and memorable events. However, people put the same readily available information on social media often times making it available to the general public. We propose an experiment to empirically validate the previous premise as well as develop an algorithm to generate passwords based off participant's Facebook public information.

Keywords: social media, passwords, entropy, password generation

INTRODUCTION

Passwords are the most commonly used, yet, inherently weak, form of authentication (Shay et al., 2010). Due to the weakness of text-based passwords, the goal of many hackers is to devise the password of a user with dictionaries of commonly used passwords. People often employ a commonly-used password because it is easy to remember (Gaw & Felten, 2006). Specifically, these passwords are memorable because they are created using information that is readily available to the person, such as family names, pets, important dates, and favorite locations (Sasse, Brostoff, & Weirich, 2001; Brown, Bracken, Zoccoli, & Douglas, 2004; Notoatmodjo & Thomborson, 2009). In today's usage of social media, people completely or

partially disclose such information publicly. This leaves organizations and personal accounts more vulnerable to password cracking than in previous years.

If organizations and online websites with personal accounts can recognize when passwords are being generated based on personal information, they can implement safeguards to help people create better passwords. In this work-in-progress paper, we propose generating a specialized dictionary that consists of passwords based on personal information gathered from a specific user's social media account. We posit, and plan to empirically test, that a person's usage of social media weakens system security by inadvertently revealing the components of their password. The remainder of this paper contains the theoretical background behind user password generation, an algorithm capable of generating passwords using publicly available personal information, and our proposed experiment.

LITERATURE REVIEW

Prior research on passwords has assigned a range of password strength from easy to crack (weak) to difficult to crack (strong). Passwords are weak when they have low entropy–a calculation involving the character space and the number of characters chosen in a password (Biddle et al., 2011). Passwords with low entropy contain less than eight alphanumeric characters, do not mix upper and lower case characters, or lack at least one non-alphanumeric character (Brown et al., 2004). On the other hand, high entropy passwords meet all three of these criteria. Entropy reduces the likelihood of success and decreases the speed of dictionary and brute forces attacks. Unfortunately, people have difficulty generating high entropy passwords that has lead to research on system attitude towards authentication systems, password generation techniques, and password memory.

User attitude towards an information system correlates with password strength. It is reasonable to believe that people want to protect system access in the most secure manner. However, a relationship between password strength and data sensitivity is not empirically supported (Zviran & Haga, 1999). Instead, password strength varies according to the user's attitude towards the authentication system. Users generate weak passwords when an authentication system is difficult to use, users are forced to create new passwords frequently, or they perceive the authentication system as an ancillary task that impedes their ability to tend to a primary task (Adams & Sasse, 1999; Brostoff & Sasse, 2001). Additionally, users believe their decision to use weak passwords is rational after they have considered the costs of entering a strong password (Tam, Glassman, & Vandenwauver, 2010). Users find the direct costs from an attack to be small and uncertain, and the indirect costs of increased creative effort and reduced memorability to be immediate and known (Inglesant & Sasse, 2010).

Users construct passwords based on information that surrounds their daily lives (Zviran & Haga, 1999). Across multiple studies, a majority of users have been shown to have a password consisting of their own name or nickname, names of family members, pet names, important dates, and important events (Brown et al., 2004; Gehringer, 2002; Vu et al., 2007; Zviran & Haga, 1999). People use this readily available information to create passwords because it makes them easier to remember (Charoen, Raman, & Olfman, 2008; Nelson & Vu, 2010).

Passwords are becoming increasingly difficult to remember because of the number of personal and work-related accounts that require passwords (Brown et al. 2004; Gaw & Felten 2006). Since users struggle to remember all of their passwords, they resort to poor password habits. The most frequently cited habit is reusing the same or similar password for multiple systems (Brown et al., 2004). For example, users may change their password from bb123#123 to

bb321#321. Other poor password habits include recording passwords on paper or electronically and sharing passwords with family members (Shay et al. 2010; Singh et al., 2007).

A technique to create memorable and secure passwords is mnemonics, which combines the first letter of each word in a phrase to create a password (Jenkins, Grimes, Proudfoot, & Lowry, 2014; Oghenerukevbe, 2010). Although mnemonics are not in the dictionary, people still use identifiable information to create mnemonic passwords.

People post the same personal information used to generate passwords on social media. The practice of divulging key elements of passwords on social media lowers the entropy of passwords because the search space the password becomes smaller. This research aims to discover whether the personal information people disclose on social media is also the same personal information people use for password generation. We posit that if this is true, people are making passwords easier to crack and increasing personal and organizational vulnerability. The remainder of the paper describes a design science and behavioral study to test this proposition.

METHODOLOGY

To test the premise that social media is weakening passwords, we propose an experimental study where 1) participants will allow us access to their Facebook account and 2) we will use that information to generate a list of potential passwords that the participant is currently using or has used in the past. We will verify with the user whether the list of potential passwords contains any past or present passwords.

We will recruit participants from a university student pool and provide course credit for their participation. We will require participants join a Facebook group, created by the experimenters, that is specific to this study. When participants connect with the group, the experimenters will receive access to the participant's About screen. The About screen can

contain sensitive information regarding the participant such as age, dates and locations of significant events (e.g., birth and marriage), and current relationships.

After the participant connects to the Facebook group, we will ask participants for their Facebook name and submit it to a script that will coordinate with our server to scrape their About page. We will take the information from their Facebook page and process it with our password generation algorithm. Although the algorithm is still in development, the final product will generate password guesses that combine names, dates, and personal interests with other common password elements such as punctuation or special characters. For example, if a participant was born in New York City in 1990 a few passwords include: NYC1990!, NYC_1990, and N3wY0rk90.

We propose a backtracking-based algorithm to generate the set of possible passwords based on the values of some publicly available personal information. Algorithm 1 (Pseudocode) shows that given some parameters (e.g., a list of strings derived from Figure 1, maximum number of strings used in the password), a list of candidate passwords can be generated by permuting the strings and special characters (e.g., &, $, #, @) in a recursive manner.

As our study proceeds, we will propose more advanced password generating and ranking algorithms. The outputs of the algorithms (e.g., ranked list of passwords) will be integrated into behavioral studies. We will also contribute to the development of new password generating and ranking algorithms through empirical analysis. For instance, we will ask users to prioritize the categories of publicly available information in the experiment based on likelihood to be used in a password and thus facilitate the design of measures for ranking passwords.

Algorithm 1 PassGen(L, i, N)

Input: List of Strings (from selected fields) L and its total number of Strings N; Maximum number of Fields (Strings) used in the a Password Max; i=1;

Output: A list of Candidate Passwords

```
if i==N then
    for the first Max Strings in L do
        Concatenate the current String S
        if S.CharAt(0)!=&, $, #, @, etc. AND number of concatenated Strings ≤ Max then
            Return S (Partial Combinations)
        end if
    end for
    if S.CharAt(0)!=&, $, #, @, etc. AND number of concatenated Strings ≤ Max then
        Return S (Full Combinations)
    end if
end if
for j=i:N do
    Swap the ith string and the jth string in L
    Return Strings derived from PassGen(L, i + 1, N) (Recursion)
    Swap the ith string and the jth string in L
end for
```

Once the password algorithm has created a list and ranked them as to the most probable, we will direct the participant to a series of pages with lists of passwords. Each page will contain 50 passwords. For each page, we will ask the participant:

- How many of the passwords on this page have you used in the past?
- How many of the passwords on this page are you currently using?
- If you have never used any of the passwords on this page, find the one most similar to a current or past password of yours. Using the most similar password, how similar is it to a current or past password?

The participant will answer these questions regarding ten pages of 50 passwords. Therefore, the participant will view 500 generated passwords. The questions the participant

answer about the passwords will create an accuracy rate for the algorithm. We will use this accuracy rate as a measure for how much social media decreases the strength of passwords.

CONCLUSION

In this work-in-progress paper, we proposed a design science artifact and a behavioral study intended to test whether people reduce their password strength by disclosing personal information on social media. The literature shows that people generate passwords based on personal information that is available to them. People disclose this same personal information on social media sites. Therefore, by collecting personal information from the social media sites, we should be able to develop an algorithm to search for passwords based on that personal information. We hope to share more findings at the workshop.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 41–46.

Biddle, R., Mannan, M., Van Oorschot, P. C., & Whalen, T. (2011). User study, analysis, and usable security of passwords based on digital objects. *IEEE Transactions on Information Forensics and Security*, *6*(3), 970–979. doi:10.1109/TIFS.2011.2116781

Brostoff, S., & Sasse, M. A. (2001). Safe and sound: A safety-critical approach to security. In *New Security Paradigms Workshop* (pp. 41–50). doi:10.1145/508171.508178

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, *18*(June), 641–651. doi:10.1002/acp.1014

Charoen, D., Raman, M., & Olfman, L. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice and Action Research*, *21*(1), 55–72. doi:10.1007/s11213-007-9082-4

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06* (p. 44). doi:10.1145/1143120.1143127

Gehringer, E. F. (2002). Choosing passwords: Security and human factors. In *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No.02CH37293)* (pp. 1–5). doi:10.1109/ISTAS.2002.1013839

Inglesant, P., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1–10). doi:10.1145/1753326.1753384

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring

password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 196–213. doi:10.1080/02681102.2013.814040

Nelson, D., & Vu, K.-P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior*, *26*(4), 705–715. doi:10.1016/j.chb.2010.01.007

Notoatmodjo, G., & Thomborson, C. (2009). Passwords and perceptions. In *Conferences in Research and Practice in Information Technology Series* (Vol. 98, pp. 71–78).

Oghenerukevbe, E. A. (2010). Mnemonic passwords practces in corporate sites in Nigerian. *Journal of Internet Banking and Commerce*, *15*(1), 1–11. doi:10.1007/978-3-531-92534-9_12

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": A human-computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131. doi:10.1023/A:1011902718709

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., … Cranor, L. F. (2010). Encountering stronger password requirements. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10* (p. 1). doi:10.1145/1837110.1837113

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Password sharing: Implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 895–904). doi:10.1145/1240624.1240759

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244. doi:10.1080/01449290903121386

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L., Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human Computer Studies*, *65*(8), 744–757. doi:10.1016/j.ijhcs.2007.03.007

Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, *15*(4), 161–185.