Discussing different approaches of how to get users to create more secure passwords: password policies, password strength meters and graphical passwords

Sebastian Gavra

Abstract—This paper gives an insight on the current developments of user’s passwords. The introduction and the second section show the problems of how users create passwords, which structures are the most common and how secure people believe their passwords to be. Regarding this information, it is safe to say that users need to be guided to create stronger and more secure passwords and it is also very important to decrease usability as little as possible. The paper presents three different approaches on how to get users to create more secure passwords. The section about password policies presents a paper-based survey of 470 participants and a large-scale two part online study of 5000 participants. The section about password strength meters presents a two part online study of 2931 participants. The graphical password section shows the results of a smartphone application of 2318 unique devices. Related work has been cited. The benefits and drawbacks of these different approaches are being discussed. The conclusion shows how these approaches can be helpful for system administrators.

Index Terms—usable security, passwords

1 INTRODUCTION

In today’s modern life, people have to use multiple passwords every day to protect their accounts and devices from unauthorized access. Users are supposed to use a different password for every account. Memorizing every single one of them can be a hard challenge for users. In order to remember their passwords, users tend to keep their passwords very simple and base them around names or dictionary words, write them down electronically or on paper and share them with others. These habits can result in low password security and users should be reminded about this problem and should be presented with alternatives. Three approaches will be discussed in section 3, 4 & 5.

2 PASSWORD COMPOSITION

In 2007, Florêncio et al.[3] conducted a large-scale study with over 500,000 participants:
The average number of sites sharing a password was 5.67. Users employ weak passwords on multiple sites when the password rules are lax. Passwords using only lowercase letters dominated at all lengths. Even if users are forced to use stronger passwords, it appears that they use longer lowercase passwords and use uppercase and special characters hardly at all. Lowercase-only accounts for 78% of the cases. The situation appears to be changed only when a site forces password policies that use a greater number of character classes. Very few users used a special character unless instructed to do so.

In 2011, Komanduri et al. [4] conducted a two-part online study of 470 participants and a large-scale two part online study of 5000 participants. The section about password strength meters presents a paper-based survey of 470 participants and must not contain dictionary words. Dictionary words and must not contain dictionary words.

3 PASSWORD POLICIES

3.1 Definition

Password policies are forcing the user to create a password which meets the policy’s requirements in order to benefit from better security. System administrators enforce users to create a password with a minimal complexity. The password must e.g. exceed a minimum amount of characters, contain numbers, upper-case letters and symbols and must not contain dictionary words.

3.2 Changing a password policy at a university

In 2010, a stricter password policy was applied to the student’s accounts at Carnegie Mellon University (Pittsburgh, Pennsylvania). Shay et al. [5] conducted a paper-based survey of 470 participants who changed their passwords.

These developments show that users should be forced and/or encouraged to create stronger passwords. The following presents approaches and discusses their benefits and drawbacks.

3.3 Users creating a password under different policies

In 2011, Komanduri et al. [4] conducted a two-part online study with five different conditions (5,000 participants). These conditions differed in length (basic8, basic16), dictionary checks (dictionary8)
and numbers of character classes (comprehensive8):

Increased entropy often correlates with decreases in usability. basic8 and dictionary8 do not provide significantly different levels of entropy, although the dictionary check provides additional protection against heuristic cracking but also adds to user frustration. dictionary8 had significantly more difficulties creating a valid password and found the process to be more difficult and more annoying. Surprisingly, basic16 provided significantly more entropy than comprehensive8. basic16 is easier to create, reportedly easier to remember and less likely to be stored than comprehensive8. While comprehensive8 is worse on every usability measure than either basic8 or dictionary8, basic16 is not. The basic16 condition proved reasonably comparable to dictionary8 in terms of password creation, storage, and reported memorability, although it did perform worse in user sentiment. Overall, therefore, using basic16 rather than dictionary8 provides a strong gain in resistance to brute force attacks at a small usability cost. Storage is correlated with the use of higher-entropy passwords. Dictionary checks, although otherwise useful, add much less entropy than expected. Adding numbers to password is thought to add little entropy, but contrast, a lot of entropy in numbers was found. Unexpectedly, users typically create a password that exceeds the minimum requirements, thus increasing password entropy.

3.4 Benefits & drawbacks
The key of an optimal password policy is high security with minimal user frustration. The approach of trying to get users to create a decently, minimal secure password like basic16 or comprehensive8 has shown that basic16 is overly superior regarding creation, memorability and and storage with similar annoyance. Users feel more secure when creating a password under a password policy.

Most users were annoyed when applying/ creating a password to password policies and some users had difficulties in meeting the requirements.

4 PASSWORD STRENGTH METERS
4.1 Definition
Password strength meters indicate the strength of a password as entered by a user in a text field, in graphical (e.g. colors: red = weak/ not meeting requirements, green = good) or text form (e.g. "Consider adding a number").

4.2 Users creating a password under a policy with different meters
In 2012, Ur et al. [6] conducted a two-part online study on password strength meters with 15 different conditions (2,931 participants).

Every participant had to create a password that met the requirements of the password policy, at least 8 characters and was assigned to one of the 15 different password meters.

1. Control conditions:
   No-meter, Baseline meter
2. Conditions Differing in Appearance:
   Three-segment, Green, Tiny, Huge, Text-only
3. Conditions Differing in Scoring:
   Half-score, One-third score, Nudge-16, Nudge-comp8
4. Conditions Differing in Multiple ways:
   Text-only half-score, Bold text-only half-score, Bunny

Password strength meters led users to create longer passwords and add additional character classes. Stringent password strength meters (e.g. one-third-score) seemed to push users to hard so users might give up on creating a more secure password. Tweaks to the password strength meter’s visual display did not lead to significant differences in password composition or user sentiment. An important factor seemed to be the combination of text and visual indicators. In the presence of password meters, participants changed the way they created a password, the majority in the stringent conditions changed their password during creation. Meters seemed to encourage participants to create a password that filled the meter. If that goal seemed impossible, participants seemed content to avoid passwords that were rated “bad” or “poor”. Meters whose estimates of password strength mirrored participants’ expectations seemed to encourage the creation of secure passwords, whereas very stringent meters whose scores diverged from expectations led to less favorable user sentiment and increased likelihood that a participant would abandon the task of creating a strong password. Wide-scale deployment of more stringent meters may train users to create stronger passwords routinely.

4.3 Benefits & drawbacks
Password strength meters help the user to get immediate feedback about their created password and encourage them to make their password longer and more secure. Stringent password strength meters can teach the user interactively how to create a more secure password. Most users did not feel annoyed using a password strength meter.

When password strength meters are too stringent, users create similar passwords like when a “normal” stringent password strength meter is used but this comes with significantly higher annoyance and frustration.

5 GRAPHICAL PASSWORDS
5.1 Definition
A graphical password is an authentication system which focuses on visual information. The user’s input is retrieved by clicking/ tapping on graphics.

5.2 Results from a smartphone application
In 2015, Alt et al. [1] conducted a study where participants used a smartphone application for 12 months. The application was released on the Google Play Store and installed on 2318 unique devices.

Participants chose the right part (46%) of images more often than the left (26%) and the middle part (28%). There was no clear tendency for the vertical distribution. Users tend to start the top right corner. 34.2% of password points were in the salient region (it covered 21.8% of an image on average). Human attackers performed about 50% better than saliency masks.

5.3 Benefits & drawbacks
Users can memorise images better than text. Graphical passwords are easy to remember and hard to guess. They are resistant to dictionary attacks and brute-force attacks.

Password registration and log-in process may take longer. Graphical passwords take more storage space than text. They are vulnerable to "shoulder surfing". [2]

6 CONCLUSION
Password creation is a problem and users need to be guided while minimizing annoyance and frustration and increasing password security. This paper showed the benefits and drawbacks of three different approaches of how to get users to create stronger passwords.

Password policies ensure the system administrator that passwords have a minimum amount of security. Users like longer passwords better than having to use multiple character classes. This preference does not have a bad impact on the password’s entropy. The stricter the password policy, the more annoyance and frustration for the user.

Password meters can be a useful tool for system administrators because users chose a password with significantly higher entropy and provide the user with an alternative to password policies with less annoyance and frustration. The best password meters should be stringly, but not too stringly, because this only decreases usability.

Graphical passwords are a promising alternative because they are easy to remember and resistant to dictionary and brute-force attacks.
REFERENCES


