Zane R. Cochran

CS 6451: Elevator Pitch

16 Oct 2013

Democratizing Password Renewal Policies Through

Enhanced Generation Feedback and Incentives

The current landscape of generating and protecting user passwords has become a veritable minefield of challenges that has led many to question the usefulness of using passwords as a security measure at all. As hackers gain access to large password databases and decrypt them with increasing success, institutions have begun placing increased responsibility on their users to create and maintain complex passwords. In addition to enforcing a variety of intricate character-based password requirements, many institutions also enforce a limited lifespan on passwords, requiring users to generate new passwords at set intervals. This research study will summarize common password protocols and address their issues through the introduction of a system of flexible password requirements that explores the tradeoffs of password complexity and password lifespan. It will seek to answer this question:

How will users modify their behavior while generating passwords when presented with the choice between simple passwords that must be regenerated frequently or complex passwords that must be regenerated infrequently?

By enabling users to see password complexity as a function of password lifespan, we can better understand how users weigh the competing interests of simple versus secure passwords.

When an institution's user database is compromised, a race begins between the hacker and the institution's users. The time required to decrypt a password can vary between minutes and years, depending upon complexity. As such, users who choose simpler passwords are more quickly vulnerable to attack than users with complex passwords. While no password is invincible to these attacks, complex passwords are favorable because it gives institutions ample time to alert users of the breach, and users enough time to change their passwords. Because of the increased occurrences of such incidences, institutions have responded by requiring users to create more complex passwords that are difficult to remember and must be regenerated at regular intervals, usually between every month to 6 months. The effort to create a password of such complexity so frequently can create a tense relationship between users and the institution, often times resulting in users writing passwords down and leaving them on their desk. Thus the struggle between institutions protecting user data and users remembering passwords goes on. The system proposed in this study will ease this tension by providing users with enhanced feedback regarding the complexity of their passwords and allowing users to tradeoff password simplicity with frequency of password regeneration.

Currently, institutions provide users with minimal feedback concerning the complexity of their passwords. Frequently they use a Likert scale-type system ranking passwords from "Very Weak" to "Very Strong." The difficulty with these systems is they lack transparency and context to users unfamiliar with the heuristic used by the institution for determining password strength. The proposed system, however, will quantify this feedback by displaying two pieces of information. Firstly,

the system will display the amount of time the password will be usable on the system. Institution administrators will be able to determine a range of lifespans such that simple and easily cracked passwords will be assigned a minimal lifespan on the system whereas more complex passwords will last much longer before they must be changed. This will allow users to explore passwords that have a lifespan that is comfortable for their usage patterns but also meets their ability to memorize.

To study the effectiveness of the system, we will deploy pre- and post-study surveys to gauge users' attitudes and behaviors toward creating passwords and their possible methods for recalling passwords. We will take particular interest in methods that have particular weaknesses, e.g. reusing passwords across multiple accounts, writing down passwords, passwords that are vulnerable to dictionary attacks, etc.). Additionally, we will ask users about their general awareness regarding password complexity and the amount of time required to exploit passwords. The desired outcome of the system will be to improve people's attitudes regarding security by giving them greater flexibility in generating passwords, as well as reducing the incidence of negative methods of password recall while improving awareness of password exploitation.

Ideally, this study will last 6-12 months, allowing the users at participating institutions to work through numerous password regeneration cycles. During this time, the system will collect metadata about individual user passwords, tracking their behavior through each password generation session to observe if their behaviors change over the course of the study. We will monitor password selection in regard to complexity and lifespan, as well as the amount of time spent generating

an appropriate password and the number of password reset requests made over the life of the experiment. While this study is ongoing, a control group will use the institution's current password system to provide data that can be used to demark the effectiveness of the proposed system.

One obvious concern this study cannot address is the prevalence of users writing down complex passwords and posting them near their computers. While this system will potentially aid in preventing external attacks, it can be difficult to prevent internal breaches of security when users post their passwords in plain sight. The hope of this study is that by introducing an incentivized password generation system, users who would normally create complex passwords and write them down, will instead create shorter passwords and regenerate them more frequently.