Putting Your Passwords on Self-destruct Mode: Beating password fatigue

Huascar Sanchez Ph.D. and John Murray Ph.D.
Computer Science Laboratory, SRI International
Menlo Park, California, U.S.A.
[huascar.sanchez | john.murray]@sri.com

Overview

Many people feel overwhelmed by the number of Web accounts they need to access on a regular basis, because of the quantity of passwords that have to be updated, especially in the context of many frequent password change mandates. This sense of challenge has been referred to as Password Fatigue (Hayday 2011) and is essentially defined as simply having too many passwords to remember (or deal with) on an erratic schedule and/or inconsistent basis.

People who suffer password fatigue are simply too exhausted from all the passwords they have to remember and all the work it takes to keep them up to date. Although there exist shortcuts and some handy tools for automating this process (Ross et al. 2005), at the end of day, it all comes down to people's own time and attention. Both of which are in short supply.

Beyond the stress it causes, the danger of password fatigue is primarily the habits it fosters when people are too distracted by all this password management (Peterson 2016). Because of password fatigue, people often adopt habits that can compromise the privacy and security of their own protected information (de Joode 2012). For instance, people tend to use a single password to access all their protected information. They do that because it is convenient for them as they only have to remember one sequence of characters. The problem with this, of course, is that if a person's password is compromised, then hostile individuals can access that person's online property unhindered. Other risky approaches include writing passwords down and storing them somewhere on one's computer, or choosing passwords that are easy to remember (and therefore easy to guess).

As time pushes us into this age of overwhelming numbers of Web accounts and passwords (Florencio and Herley 2007), it will be important to figure out ways to deal with password fatigue without overwhelming users. In an attempt to address this problem of password fatigue and other unsatisfactory issues surrounding password-based security, we explore the idea of self-destructing passwords.

Passwords are not supposed to be convenient or permanent. The best passwords are impossible to remember and temporary. Hanging onto them increases the chances of them falling into the wrong hands, so self-destruction makes a lot of sense. We therefore examine the concept of ephemeral content and how this notion relates to passwords and password fatigue.

Ephemeral content

Technology has given us immense storage capabilities. However, this digital space has grown beyond our consumption capacity -- both physical and mental. We simply store more data than what we really need and are capable of dealing with. Ephemeral content (Shein 2013) can help us deal with this growth of digital space. Not only it can help us reduce our digital footprint, optimize our storage capacity, but also ensure the privacy and security of our protected data. Ephemeral content is simply content that disappears.

Many will remember the catchphrase “This message will self-destruct in five seconds” used in the *Mission Impossible* television and film series. This catchphrase is a good example of how ephemeral content can limit the threats of one's data from falling into the wrong hands.

Along these lines, we can think of many other instances when it would be preferable to have passwords auto-deleted once they have been used them in the appropriate manner. For example, suppose a person was affected by Apple's celebrity breach and now they have to change their list of 300+ IDs/passwords to prevent some unauthorize access. Or perhaps the person could not remember the master password to the list of 300+ IDs/passwords. Another possibility is that they had experienced another password change mandate and have to search the entire list of passwords to keep it up to date. These are the type of instances that lead to password fatigue (Hayday 2011). Consequently, placing a shelf life of passwords is a viable solution for addressing this problem.

Implementing self-destructing passwords

Implementing systems for self-destructing content is non-trivial (Roesner et al. 2014; Geambasu et al. 2009). The problem, however, is that each system requires users on both ends of the solution to install and setup a new application.

For self-destructing passwords, on the other hand, we envision a system that only requires those who want to use self-destructing passwords to download an application. Once downloaded, they can confirm their identity using keystroke dynamics (Monrose and Rubin 2000), create a password, set its target account, immediacy and access limitations. Once they have created this password, they can go ahead and gain access to this account.

This entire process can be automated. We will only expose to the user a very familiar user interface (very similar to those user interfaces used in Web forms). This user interface, once open, will confirm the identity of the user using biometrics. Then, if the identify is confirmed, it will request the user to enter a username and a *new* password, as well as the password immediacy and access limitations. Behind the scenes, the tool will synchronize with the target Web application, making sure this self-destructing password is known by this application, so when entered, the user can gain access into that target Web account. Figure 1 outlines the flow of this self-destructing password application. Our full paper provides the broader implementation details of this approach.

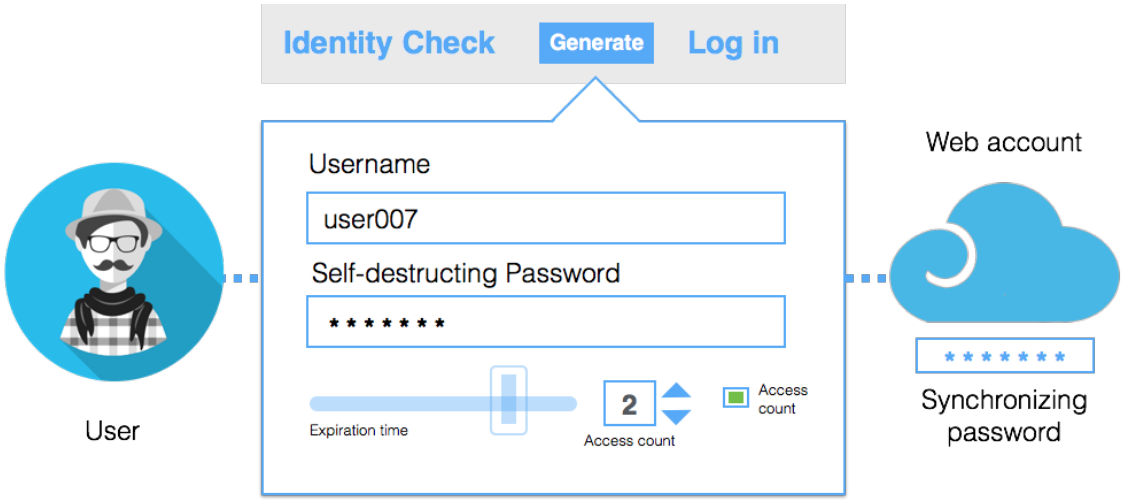

Figure 1. Self-destructing password architecture

References

de Joode D. 2012. Does password fatigue increase the risk on a phishing attack? *Tilburg University*.

Florencio D, Herley C. 2007. A Large-scale Study of Web Password Habits. *Proceedings of the 16th International Conference on World Wide Web.*

Geambasu R, Kohno T, Levy AA, Levy HM. 2009. Vanish: Increasing Data Privacy with Self-Destructing Data. *Usenix Security Symposium*.

Hayday G. 2011. Security Nightmare: How do you maintain 21 different passwords.

Monrose F, Rubin AD. 2000. Keystroke dynamics as a biometric for authentication. *Future Generations of Computer Systems.*

Peterson, Andrea 2016. Why changing your password regularly may do more harm than good. *https://www.washingtonpost.com/news/the-switch/wp/2016/03/02/the-case-against-the-most-annoying-security-measure-virtually-every-workplace-uses/*

Roesner F, Gill BT, Kohno T. 2014. Sex, lies, or kittens? investigating the use of snapchat's self-destructing messages. *Financial cryptography and data security*.

Ross B, Jackson C, Miyake N, Boneh D, Mitchell JC. 2005. Stronger Password Authentication Using Browser Extensions. *Usenix Security Symposium.*

Shein E. Ephemeral Data. 2013. *Communications of the ACM*.