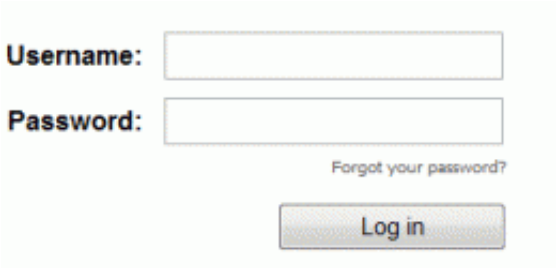
Google wants Password123 in Museum of Bad Headaches

19 January 2013, by Nancy Owano



Credit: Wikipedia.

(Phys.org)—Should typed passwords ever make their way into the Memory Bin, no tears will be shed in certain quarters at Google. The search giant is taking a serious look at a computing future where users have a safer environment that can secure their online information and accounts via physical passwords, perhaps in the form of finger rings or USB sticks or keys. Google's Vice President of Security Eric Grosse and engineer Mayank Upadhyay have presented their suggestions for better hardware authentication in an upcoming research paper to be published in *Security & Privacy* magazine.

Google has been investigating alternatives to typed passwords, which includes a Yubico log-on device slid into a USB reader as part of Google's quest to help strengthen password security. Google's eyes are on future login techniques that will be primarily device-centric. Wired, in a sneak peek at the research paper set for publication, reported that the paper explores several physical device options, to make a password process that will be easy to accommodate but also sufficiently secure.

Google's suggestions include a ring worn on the finger. and the YubiKey device from Yubico. In the YubiKey scenario, it would be programmed so that it can automatically log a user into that user's Google account. (Yubico was founded in 2007 with a prototype of its YubiKey for securing online identities. The devices are manufactured in Sweden and the U.S.)

"Along with many in the industry, we feel passwords and simple bearer tokens such as cookies are no longer sufficient to keep users safe," Grosse and Upadhyay wrote in their paper, according to *Wired*.

Their project focus is none too soon, as, beyond Google and within the general Internet community, hacker fever has turned into password-reset fatigue. Users have complained over wiped out mail accounts and stolen data from their hacked accounts. Security experts have argued that no passwords are really secure enough, and even CAPTCHA schemes to prove the user is human have been found lacking in keeping users safe.

Media attention to the password impasse grew widespread in November, when Wired senior writer Mat Honan wrote, "This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat. As a three-letter username, it's considered prestigious. And to delay me from getting it back, they used my Apple account to wipe every one of my devices, my iPhone and iPad and MacBook, deleting all my messages and documents and every picture I'd ever taken of my 18-month-old daughter."

Google's Grosse does not see the utter obliteration of the password but instead a situation where users can be freed from the need to implement and re-enter complex passwords. "We'll have to have some form of screen unlock, maybe passwords but

maybe something else," he said. Nonetheless, he added, the primary authenticator will be some piece of hardware.

Grosse and Upadhyay acknowledged that others have tried similar approaches and actually did not achieve much success in the consumer world, but the two authors of the research paper are not deterred. Success may come with wider cooperation outside Google. "Although we recognize that our initiative will likewise remain speculative until we've proven large scale acceptance, we're eager to test it with other websites."

According to *Wired*, Google has created a universal protocol for device-based authentication that is able to work independent of Google's own services; just a web browser is needed to support the standard.

APA citation: Google wants Password123 in Museum of Bad Headaches (2013, January 19) retrieved 16 September 2019 from https://phys.org/news/2013-01-google-password123-museum-bad-headaches.html