Rejoice! The End of the ‘User Name and Password’ May Be Nigh

By Christopher Matthews

May 16, 2013

What’s the absolute worst part of the Internet? Reasonable folks may disagree. One could argue pop-up ads, another might posit the endless stream of baby photos on your Facebook feed. But most would agree that keeping track of an endless string passwords ranks somewhere at the top.

Nobody, of course, can remember a unique password for the dozens of sites we each sign into each day, so we end up using the same one over and over again. But this practice makes us increasingly vulnerable to hackers who can find valuable passwords for our bank accounts and email by breaking into poorly protected sites.

A study released last month by Nok Nok labs showed that the average Internet user had 6.5 passwords, and they shared one password, on average, between 3.9 websites. Furthermore, ever-growing computer power is causing even safe passwords to be vulnerable. According to a report released earlier this year from consulting firm Deloitte, more than 90% of user-generated passwords are “vulnerable to hacking.” Reads the report:

“Most organizations keep usernames and passwords in a master file. That file is hashed: a piece of software encrypts both the username and password together. Nobody in the organization can see a password in its unencrypted form … So far, so secure. However, master files are often stolen or leaked. A hashed file is not immediately useful to a hacker, but various kinds of software and hardware … can decrypt the master file and at least some of the usernames and passwords. Decrypted files are then sold, shared or exploited by hackers.”

In recent years, the scope of this problem has become apparent as high-profile websites like LinkedIn and Gawker have suffered major breaches of their password databases. And while there are steps users can take to protect themselves, like using complicated passwords or taking advantage of two-step verification login systems, it’s clear that most users simply don’t protect themselves well enough.

This is why a consortium of tech companies, including PayPal and Google, have joined together to dream up the future of passwords. And the future, according to this FIDO alliance (which stands for Fast Identity Online) is to have no passwords at all. “Passwords are just not working terribly well anymore,” says Michael Barrett, Chief Information Security Officer of PayPal and President of FIDO. “And they’re starting to impede the development of the Internet ecosystem.”

Barrett says that the failure of the password system isn’t an immediate crisis for Silicon Valley, especially for companies that have the wherewithal to invest in robust security systems. But if the problem keeps getting worse, it will begin to erode people’s confidence in online commerce, hurting the industry all around. FIDO is an effort by the industry to get ahead of this problem and dream up a replacement to the password system before its too late.

So what is FIDO’s solution? As a consortium of companies, FIDO isn’t interested in coming up with a single alternative to passwords, but rather wants to create a technological framework through which different companies can offer alternatives to the password system. While FIDO is agnostic about what method or methods of “authentication” ultimately replace the password, Barrett explained that the technology exists for devices like computers and smartphones to recognize who you are through your unique physical qualities.

For instance, camera resolution on computers and phones is advanced enough that your computer could verify who you are by scanning your face or eyes. And Barrett expects that within a year smartphones with fingerprint scanners will hit the market. Other examples of authentication methods include touch screens that can read your signature, and voice recognition software.

If a user has one of these devices, then websites which join the FIDO system can choose which authentication methods to accept. For instance, PayPal might decide to allow users to sign in using voice and face recognition.

But biometric methods aren’t the only way users could decide to sign into websites. They could decide instead to use a combination of a password and physical object like a USB plug that would tell your device that you are who you say you are. This combination of a password and a device that you carry around with you is much safer than a simple password, and would allow the use of easy-to-remember passwords, since the account can’t be hacked unless accompanied by the physical device as well.

Barrett claims that this process of moving away from passwords will take a period of years, but says that the technology to do it is available now. It’s just a matter of websites and devices to getting together to make it work. He believes it will happen because, in the tech world at least, consumers are pretty good at getting what they want.

Says Barrett, “Consumers want something that’s easy to use and secure. Passwords are neither.”

*Original text is in the following URL:*

*http://business.time.com/2013/05/16/rejoice-the-end-of-the-user-name-and-password-is-nigh/*