Lawyers Moving Past Passwords

by Sharon D. Nelson, Esq. and John W. Simek

Passwords have been around since the early days of mainframe computing. Believe it or not, passwords were not originally designed to prove identity. The betting money is that computer passwords first showed up at the Massachusetts Institute of Technology in the mid-1960s in order to track time when using a mainframe computer: The Compatible Time-Sharing System (CTSS).

Today, passwords are used to help authenticate the identity of the computer user. From a security perspective, the problem is that people use crummy passwords, forget them and even reuse them across multiple systems. At the end of the day, if someone has your password, the computer doesn't know it really isn't you. It's no secret that many lawyers are resistant to change. Abandoning passwords is no different. With the significant increase in remote workers, get ready for a change in how you will access your firm's network or cloud service.

History

Password managers help users by generating strong and unique passwords for every account you access. Depending on the password manager you use, there may be issues with accessing the encrypted password vault across multiple devices. Many services will allow you to use your Apple, Google or Facebook passwords for access instead of creating one password specific for their service. That strikes us as a bad idea. If their service is compromised, the attacker has keys to your Facebook, Google or Apple account. You can add two-factor authentication (2FA) to increase security, but there are ways to intercept the second passcode sent by a text message.

Going Forward

You've probably heard of multi-factor authentication. A password is something you know. A second factor is something you have, such as a security key or token. A third factor is something about you – biometrics. There is a move afoot to totally ditch passwords and move to something you have and something you are.

Fast Identity Online (FIDO) are standards designed to let you dump passwords as an authentication method. The standards utilize hardware security keys and dovetail with biometrics. Think of hardware security keys as the digital equivalent of your house key. The security key plugs into a USB or Lightning port. It is a single device that works with multiple apps and websites. The key can be augmented with biometric access such as Windows Hello or Apple's Face ID.

Andrew Shikiar, executive director of the FIDO Alliance said, "Within the next five years, every major consumer internet service will have a passwordless alternative. The bulk of those will be using FIDO."

FIDO will stop phishing since it only works with legitimate websites and not the bogus sites trying to get your credentials. Stolen passwords won't be effective either since the attacker won't have the security key. If FIDO is successful, firms might not require passwords at all.

FIDO Process

When you visit a website login page, you insert your hardware security key (e.g. YubiKey) and then use biometric authentication such as Apple's Touch ID or Windows Hello. As an alternative, you can also use your smartphone as a security key. The process starts the same way by entering your username. You will then get prompted on your phone. Unlock the phone and then validate yourself using the phone's biometric authentication system.

What Could Go Wrong?

Passwords have been around for a long time and it will be difficult to switch over to security keys. The reality is that setting up security keys is a heck of a lot harder than picking a password or having your password manager do it for you. The primary difficulty is because the various websites use different procedures to register and use your hardware keys. As an example, Twitter only lets you use one security key and doesn't allow a backup key. In other words, there is no consistent process that is the same across all sites. Another issue is that a site may not support the hardware key that you own. That means you will have multiple hardware keys in to access the various required sites.

The hardware keys cost money too. That means there will be potential pushback from users due to the investment. Finally, keys can be somewhere you are not, broken, stolen or lost.

Reality Prediction

We do believe that passwords will ultimately go away, but it won't happen in the near term. It will be a slow process for users to let go of the familiarity of passwords. We predict that FIDO implementations will take at least five years (perhaps longer) to become commonplace.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com