LegalInk magazine

TWO-FACTOR AUTHENTICATION: A PASSWORD EVOLUTION

Why do we need passwords? They are ubiquitous and in our faces all day. I log in on 200 to 300 websites, routers, firewalls, computers and phones during an average day. Using passwords is still considered a best practice to secure these systems. However, as I will show, passwords alone cannot be the be-all end-all for security. Our password systems must evolve to better protect our digital identities.

In the Beginning…

To understand where we are today, it is useful to take a quick look at the past. When computers first came onto the scene, they were big and bulky machines, and the people who worked on them comprised a small group. The need for security within the group was similarly small. As long as physical access to the terminal was restricted, that security was enough. Everybody knew everybody else.

As computers grew more powerful and networks expanded, the people working on these systems could not be sure who was accessing their system. A master database of user accounts was created, and that master issued user IDs and passwords. The end result for the computer system was better security and control of resources. This introduced the need for users to remember passwords, though. Unfortunately, it often happened that when a fellow engineer needed access and didn't have a password, one would be shared, which led to security problems.

With the modern power of computing and our interconnectedness via the internet, we frequently see systems being compromised. The notable computer security hacks that dominate the headlines bear witness to this. These targets are so enticing because the systems they use do not allow for true identification of the end user.

In our computer systems, a user ID and password are really a digital representation of ourselves. The system understands the password as an object within the computer system database, and that object has certain rights to resources. As long as the proper credentials are given, the computer system will grant access to the object. But the system doesn't know that the GSmith account is actually George Smith. It only knows that some entity presented the proper credentials.

Computer passwords have evolved, and this progression changes how we work with our digital identities. The whole password concept started small, with a single identifier. Then it evolved into requiring user IDs, then requiring separate passwords, then auditing of access and on and on. This evolution will never come to an end as new systems and new thinking emerge. One particular aspect that does not seem to stop is the continued compromising of computer systems. Our current systems need additional evolution to counteract incursions.

So where does this leave us? What will passwords look like in the coming years?

One current method of authentication involves requiring a second authentication. Essentially, a second credential is needed to identify the resources being accessed. In computer terms, this is called two-factor authentication, or 2FA.

How does 2FA work?

The process involves challenging the user after the password is given with a request to present a physical token, such as an RSA or YubiKey. Without the physical token, access is denied. If the main password is compromised, the resource will still be protected because only true users will have a physical token.

How does that user manage multiple passwords and tokens? There are several current password managers on the market that can help. They work by having a central database, aka the Password Manager, and instead of that database managing access for only internal resources, it also manages access for external resources. The Password Manager has the ability to change passwords for all the resources it oversees. The user protects the Password Manager with a password and two-factor authentication, a physical token they possess.

Another method is using proxy access to verify passwords. In this example, a website trusts logins from a second website to authenticate its users. A prime example of that is the Facebook Login. This allows a website developer to trust Facebook for authentication requests and pass the credentials through. You also see this with Active Directory Federation Services for integrating your Active Directory credentials.

As we continue to move forward, not only do we need to evolve our computer systems, but also our security. Passwords represent the easiest method to identify our digital selves. With so much of our society based on password credentials, it behooves us to evolve how we think about passwords and security.

About the Author

Michael Paul is the chief technology officer at Innovative Computing Systems and has over 15 years of experience in the legal field. In his current role, along with evaluating new technologies and designing various systems around providing these solutions to the legal community, he also provides the glue for the internal technology ICS uses. Paul holds a bachelor's degree from Northern Arizona University and lives in Southern California with his family.

Originally published May 12, 2017 by Legal Ink Magazine, http://legalinkmagazine.com