The Knowledge Bank™
EXCLUSIVELY AT www.srsnodgrass.com
"Your Key to a Wealth of Information"
SNODGRASS
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

THE END OF PASSWORDS: THE FUTURE OF AUTHENTICATION

As seen in the December 2009 Issue of Community Banker

BY JEREMY BURRIS, CISA, MCP, LPT, CPTS, CEH, ECSA

As traditional login IDs and passwords become easier and easier to compromise, companies seeking to secure data are looking for newer authentication methods. In five years, it's likely there will no longer be passwords.

Why? In order to provide adequate protection, passwords have become more complex. But the more complex passwords become, the more likely employees will write them down somewhere. This just turns the problem from one of logical security to one of physical security.

Passwords have other weaknesses. Backwards compatibility with software can be a problem as can software vendor settings that don't allow for sufficient complexity compared with operating system settings. Even when operating system password settings are within current industry standards, software applications may not be. This can lead to multiple passwords for different sign-ons, leading back to the need to write passwords down.

Another reason passwords are becoming passé is that they are too easy to crack. As password complexity is strengthened, password-cracking should become more time-consuming, because the computer has to perform millions of computations or attempts before it finds the correct answer. But thieves have gotten around that problem by pre-computing every possible combination ahead of time, storing the results in a database. A rainbow table, as these pre-computations are known, can almost instantaneously reveal the password. Add this tool to a good network password "sniffer" and complete network access is possible in minutes.

Keystroke Logging has become another password nightmare. Someone downloads something "by mistake" from the Internet and later discovers it sends every keystroke to a hacker in some foreign country. Every password this person types in is open to an attacker.

The Future of Authentication

So where are we headed? Authentication is beginning to rely on technologies that once seemed fictional but that are quickly becoming feasible and affordable. As biometric devices become cheaper and more widely acceptable, they will become the norm. Here are a few examples, in order of current adoption:

1. Multifactor Authentication. This common device pairs the traditional login ID and password with an image that is tied to a specific machine. If the Web site you are authenticating "sees" this image stored on a hard drive, it recognizes the user. If the image is not recognized, it redirects to a series of secret questions to further authenticate. Many of the top Internet banking companies use some type of multifactor authentication.

2. Fingerprint Scans. This requires a finger touch point where a fingerprint is read and the user is authenticated. Some of the first fingerprint scanners were heat-activated, which allowed attackers to simply breathe onto the scanner without touching it. This would lead the scanner to recognize the last fingerprint that had touched the device (which was probably an appropriate one). Most of these early problems have now been resolved. This type of biometric authentication device is becoming more common as the costs involved with implementing them have gone down.

3. Type Recognition is a relatively new (and highly accurate) form of authentication. The way each person types (speed, pressure on keys, and other identifiers) is unique, almost like a fingerprint. As a user types in several lines of text, the computer can learn to identify the user's unique typing style. To authenticate, the user types in a pass phrase long enough for the system to recognize the unique style of typing that was previously established.

4. Retinal Scanners are similar to fingerprint scanners. Using a low-grade laser or similar device, they can identify the uniqueness of a person's retina (in the eye). These devices are still in the early stages of development and are still costly, but they are slowly making their way into common use.

These are some of the more likely authentication devices of the future, but there are many new ideas that will enable us to better protect our networks. Because traditional login IDs and passwords have become easy to compromise, more secure authentication will move towards biometric and multifactor authentication devices. These devices will come with their own challenges (both for the user and the attacker) but should ultimately provide better security.

About the Author

Jeremy Burris is a senior technology services consultant at S.R. Snodgrass, A.C. His areas of expertise include network attack and penetration and other IT audits for financial institutions and private companies. To view articles and video presentations on banking-related topics, visit Snodgrass' Knowledge Bank at www.srsnodgrass.com

This newsletter is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this newsletter, the information contained herein should not be acted upon without professional advice related to your specific situation.