Paring password pileup

Firms working on streamlining security, from fingerprints to smart cards / **Simson L. Garfinkel**

PASSWORDS ARE THE digital keys that unlock the resources of today's computer networks. If you access the Internet at all, then you almost certainly have a password that logs on to your on-line service, a password that gets your electronic mail, and many others to access Web sites, your bank account, your on-line brokerage, and those ubiquitous multi-user games. Your computer at home may even have its own password – handy if you have files you don't want other members of your household getting into.

Passwords have been a part of computer security for more than 30 years, mostly because they are relatively easy to use and don't require special hardware. But passwords have a fundamental catch: To remain secure, they must remain secret. Unfortunately, there are many ways your password can be easily revealed to people who mean you harm.

Miscreants can figure out your password in many ways. You might make the mistake of picking a password that is easy to guess, such as "password," "secret," or your spouse's first name. Even if your password is hard to guess, you might share it with somebody, who in turn shares it with somebody else.

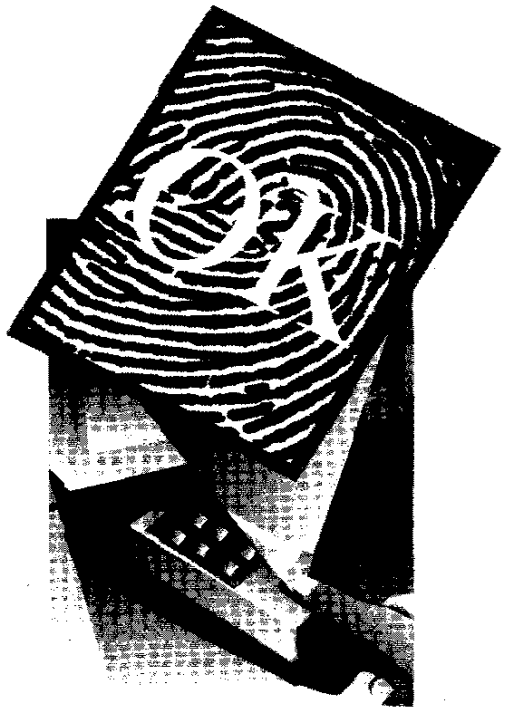
Sometimes con artists simply call you up or send you e-mail asking for your password. Someone posing as a technical support person, for example, might inform you that there is a problem with your account, and they need your password to fix it. Whatever you do, don't give your password to anyone. Technical support staff should never need your password to fix systems.

Passwords are also a pain because most of us have so many of them. Most people I know have at least a dozen passwords, codes, and PINs that they have to use every week.

Companies around the world are working hard to make passwords obsolete. One possible way to do away with them is to use the human body to identify each computer user. This is called biometric technology, and in recent years companies have tried using fingerprints, voice prints, palm prints, retina prints, iris prints, and even keyboard typing characteristics to identify individuals.

For the last month I've been experimenting with the Fingerprint Identification Unit, a low-cost fingerprint reader designed for desktop computers. My reader came with a software package created by I/O Software (www.iosoftware.com) that let me use the device to log into my Windows NT desktop workstation.

It's pretty cool to be able to sit down at your computer, press a little gizmo, and get logged in. Unfortunately, the fingerprint reader is a bit slower than a username and password. It is also less accurate: About one out of every five tries, the scanner didn't work and I had to get fingerprinted a second time. A few days into my experiment, I discovered that you need to have a fingerprint scanner connected to every computer on your network if you are going to use these devices instead of a password.



GLOBE STAFF ILLUSTRATION/ANTHONY SCHULTZ

The biggest problem, however, is that programs on my system and on Internet Web sites don't yet know how to use fingerprints, so I ended up still needing to use passwords daily.

Another approach to solving the password problem is to use smart cards. A smart card looks like a credit card but contains a special-purpose computer and a chunk of memory. The card can store a number of secret keys that can be verified by your computer or by other computers on the Internet using public key cryptography. For systems that don't know about public key "digital certificates," the card can also store conventional passwords.

To use a smart card you need a reader and special software. Litronic (www.litronic.com) sells a variety of readers for PCs and software that integrates with Netscape Navigator. The standard reader costs $139 (including a smart card and the software) and connects to the serial port on the back of your computer. A $179 reader plugs into the PCMCIA slot on the side of many laptops. Litronic is also working on a keyboard with its own smart card reader built in.

One of the nice things about using a smart card is that you can lend it to a colleague, then take it back and be assured the person hasn't made a copy. That's something you can't do with either fingerprints or conventional passwords.

Besides unlocking Web sites, smart cards can also be used for encrypting information or signing digital documents. For this reason, many businesses are considering deploying smart cards on their corporate networks.

"We have been overwhelmed with pilot requests and people deploying test networks inside their corporations," says Eric Greenberg, Litronic's chief operating officer. The firm is involved in dozens of pilots with some of the world's largest companies, he said.

Using a smart card is a little like using a bank card for an ATM. When you sit at the computer, you insert your smart card and type a PIN. (Of course, although the PIN is a code you have to remember, it can reduce the number of necessary passwords from dozens to one.)

As long as the smart card is in the reader, you can access files, unlock secret documents, and visit Web sites that use digital certificates. When you are done, just pull out your smart card and the access is gone. The card can also be programmed to erase itself if somebody steals it and tries to guess different passwords.

Today Litronic's system works only with Netscape Navigator. Ideally, you would also like to be able to use the smart card for logging on to your computer as well as unlocking other resources on the network that are not accessed through a Web browser. Greenberg says Litronic is working on such a product, which may be available this year.

Technology writer Simson L. Garfinkel can be reached at plugged-in@simson.net.