GCN
GOVERNMENT COMPUTER NEWS

Simple sign-on

05/21/07
By William Jackson

When passwords got out of hand, a California county put its finger on the problem

When the auditor/controller-recorder's office of San Bernardino County, Calif., tried to improve its information technology security through requiring complex passwords with upper- and lower-case letters and special characters, the plan backfired, IT chief Patrick Honny recalled.

"We had situations, especially after a weekend or a holiday, when our help-desk requests went through the roof," Honny said.

To avoid forgetting the long passwords, some users were writing them down, a basic security no-no.

"We did it to improve security, but were only making it worse," he said.

This is a common problem. When the city of Glendale, Calif., lengthened passwords for IT users and shortened password life, "the end users started to retaliate" by writing down and reusing passwords, said Steve Richmond, a security analyst at the city's Information Services Department. "So we decided to go for another option." For many organizations, that option is biometrics. And the most widely used form of biometric authentication is fingerprints.

Fingerprints account for 43 percent of the market, according to the International Biometric Group, a consulting company based in New York and London. Facial recognition is second at 19 percent, followed by hand geometry (9 percent) and iris scans (7 percent).

With the growing availability of small, inexpensive fingerprint readers for PCs, a number of vendors are touting fingerprints as a replacement for passwords. "We're using it strictly for password replacement," said Richmond, who is using a system from DigitalPersona.

San Bernardino County is using the DigitalPersona Pro in the recorder's office, where most users now sign on to the network with a fingerprint rather than a password.

"It's not intuitive to improve security with greater simplicity, but that's what we've done," Honny said.

Fingerprint reading is a maturing technology that — despite a long-term interest in biometric authentication — has taken some time to gain wide acceptance. In addition to software, it requires an additional piece of hardware to read the print, and the technique has negative connotations for many who associate it with criminal investigations. It has often been used as a second factor of authentication, supplementing passwords to add a layer of security to sensitive networks and applications.

However, print readers — added on or embedded — appear to be reaching a critical mass, and acceptance is growing among users happy with the convenience of shedding some of their passwords.

The growing number of laptop PCs with embedded readers also makes fingerprints a logical tool for mobile users to authenticate to wireless networks. Bio-NetGuard from Shimon Systems provides fingerprint

authentication appliances for Wi-Fi networks.

“It becomes your authentication server for the access point,” said Baldev Krishan, the company’s president and chief executive officer.

The small box connects either directly to the access point or a router to provide authentication for multiple access points. It uses algorithms from NEC, and a Texas Instruments DSP chip runs custom Shimon firmware. It supports most third-party fingerprint readers.

For Shimon and DigitalPersona, interoperability with a wide variety of print readers is the key to creating an effective authentication tool. Both companies’ solutions support optical and thermal readers from different vendors.

“We don’t care, as long as we get the image,” Krishan said.

For Shimon, there is also the challenge of interfacing with different network cards and access points.

“It’s not a trivial task,” Krishan said. “There are always subtle differences,” even though the technology is intended to be interoperable.

Both systems store a template of distinguishing characteristics of each fingerprint. Users are authenticated by comparing a fresh print image with the template. Because the systems do a one-to-one match of a fingerprint to a single stored template rather than searching for an identity, the chances of a false positive are small for Bio-NetGuard, Krishan said.

“If you had millions of users, the likelihood of a false positive could be pretty high,” he said. But with a maximum of only 250 identities stored on each appliance, the chances of a mistake are small.

DigitalPersona claims a rate for its tool of one false positive in a million tries and a false-rejection rate of 1.3 percent. The authentication engine can be tuned to make it more or less sensitive, but that is the sweet spot, said George Skaff, marketing vice president.

The reader can register as many as 10 fingers for each user, and it scans each print four times during enrollment to create the template. DigitalPersona offers its own USB-connected reader and supports most third-party readers.

It integrates with Microsoft Active Directory, and a window requesting a print scan replaces the standard Windows log-on dialog box that requests a password.

The system does not replace the password. It is an overlay that uses a fingerprint to access a password vault that is used by the system to log on. Because the user does not have to remember them, these passwords can be generated automatically and are more secure than those created by the user.

“Behind the fingerprint, we can put the most complex password we want to,” Honny said.

San Bernardino and Glendale use fingerprints for desktop PC users, not mobile users.

“We don’t have a lot of mobile users,” Richmond said. “It is for the nine-to-fiver who comes in and drops his finger on the reader every morning.”

It did not take long for the jurisdictions to settle on DigitalPersona when they started investigating password replacement three years ago.

“At the time, there weren’t a lot of options,” Richmond said.

San Bernardino also looked at retina scanning and keystroke evaluation but settled on fingerprints because officials wanted something for less than $100 per desktop PC, Honny said.

DigitalPersona Pro client software now runs about $60 per seat, with a $50 license. The server costs about $1,500.

Honny tested the product with a small group in his office, and it was simple enough that it was quickly introduced to the rest of the office with only a minimum of testing.

Users have the option of using fingerprint sign-on or retaining their password, but almost all of the 300 users opted for fingerprints, he said.

“We have one or two who refuse to use biometrics, for whatever reason,” he said. “And we have run into a bit of a problem where an individual for some reason has trouble registering a fingerprint.” This is not common, however, and tweaking the sensitivity usually solves the problem.

In Glendale, the implementation has been more spotty.

“We’re not an Active Directory shop, yet,” Richmond said. “We’re in a migration mode.”

But the fingerprint reader has become a standard peripheral as new hardware is acquired, and departments move to Active Directory in fits and starts, as budgets allow.

It’s all local

Where the Windows NT domain model is in use, credentials are stored locally on the desktop PC for local authentication only. With Active Directory, there will be a central repository to allow network sign-on.

With the technology in place, San Bernardino is finding new ways to take advantage of biometric authentication.

“It has more uses than allowing a password vault,” Honny said.

For example, one use is to enable electronic filing of documents from title companies. State law requires that all documents bear an ink-on-paper signature. A pilot program allows an authorized person at the title company to attest to the signature when filing the documents electronically, using a fingerprint to authenticate to the system.

So far, fingerprints are proving to be a workable, economic alternative to password authentication.

“It’s not a 100 percent fit, but it’s close,” Honny said.