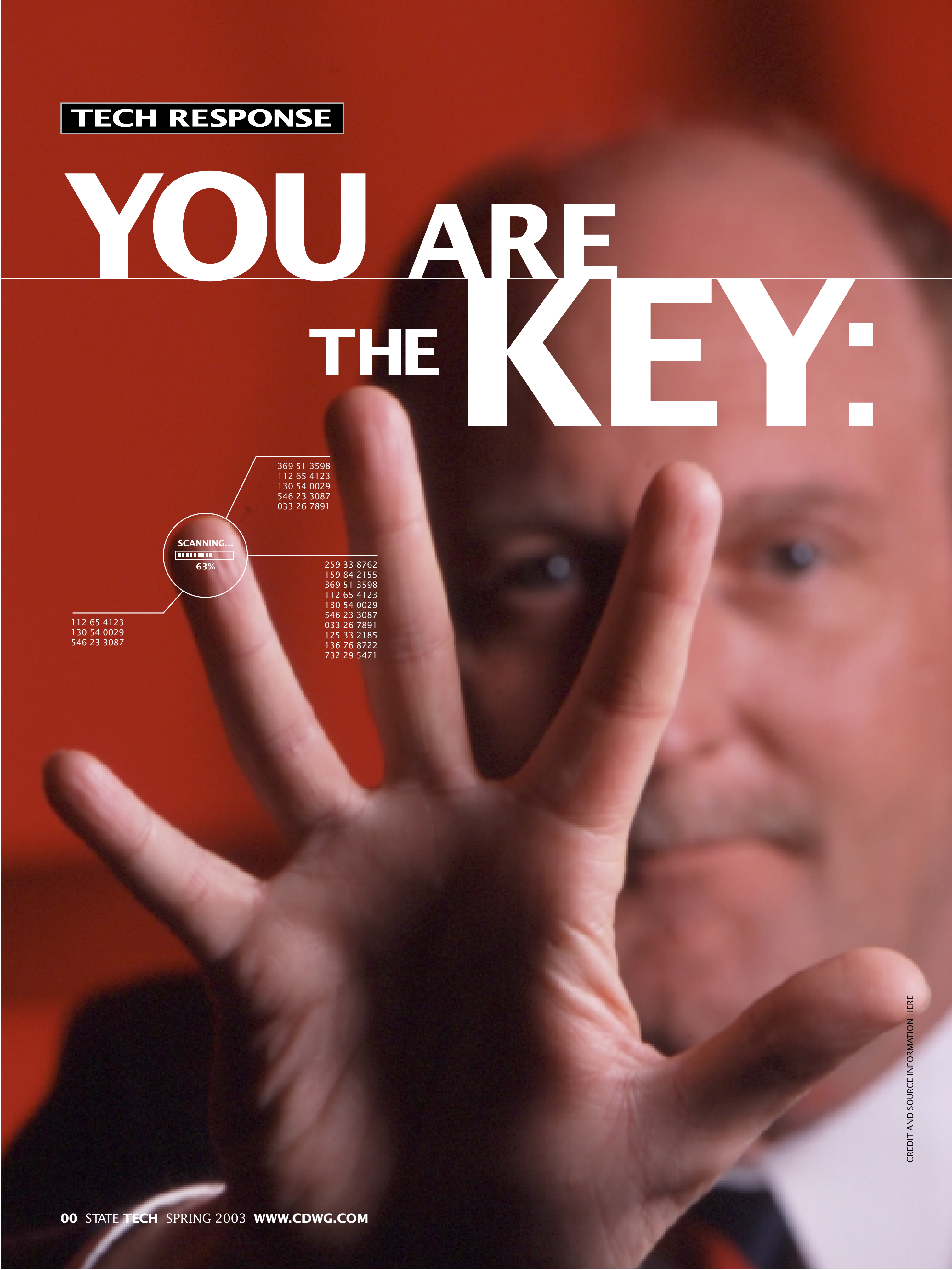
TECH RESPONSE

YOU ARE THE KEY:



CREDIT AND SOURCE INFORMATION HERE

THE MANY FACES AND THUMBPRINTS OF BIOMETRICS

DAVID SPARK

PASSWORDS may quickly go the way of the typewriter, because their inherent alterability makes their use a security risk. Unique biometric data, such as a retinal scan or fingerprint, however, can't be lost or used by anyone else. Numerous state, local and federal governments are using biometric technology for logging on, accessing secured doors and identifying individuals.

Mark Denari
SFO Assistant Deputy of Airport Security

CREDIT AND SOURCE INFORMATION HERE

Ah, there's the alert. It's time to change your password again. No worries. This should be easy. First, think of a password that's at least eight characters long. Second, make sure it meets all the necessary password security requirements. It can't contain any part of your name or company name. In addition, your password must include three out of the following four ASCII symbols: an uppercase letter, a lowercase letter, a number and a special character (such as !, % or #). Got one that fills the bill? Sorry, you used that password once within the last five forced password changes. Try again.

This irritating game of Scrabble hieroglyphics, repeated every 45 days, is a standard procedure for government employees of Tarrant County, Texas. This password-creation process seems annoying, but it's necessary. If David Plzak, the county's chief security officer, didn't enforce a compulsory set of rules, his end users in north central Texas might resort to their pets' names to access the network. Not a good option when many of your users are elected officials and judges, and such information becomes public every week in the local paper's metro section.

To alleviate some of the pressure to repeatedly come up with new complex passwords, Plzak is pushing county employees toward a biometric-based log on system to augment password authentication. Instead of creating and remembering multiple passwords, users sign on with a body part, such as a hand, finger, eye or face, to gain access to the county network.

Plzak has just begun testing biometric authentication with about 25 users, but he hopes to roll it out to most of the county's 3,000 employees by the end of this year. "It's easier to put their finger on the fingerprint reader than it is to have to remember six passwords or keep six passwords," explains Plzak. "So we've made it easier for them to authenticate themselves more securely."

Beyond simplicity, biometric log ons are more secure. Unlike text-based passwords, a biometric password can be used only by the person who created it.

0.01%

The biometric scanner is close to flawless claims Mark Denari, Assistant Deputy of Airport Security at SFO. He's had limited problems during enrollment, and estimates cases of false positives run somewhere in the neighborhood of 0.01 percent.

To use a biometric device for user authentication, you must first enroll. The enrollment process creates a biometric template. This template, a collection of unique points, is then stored locally or in an LDAP database, such as Microsoft's Active Directory, for user authentication. Even if someone successfully steals your template, the template by itself would be useless. It can be unlocked only by your body part, like a thumb. And recreating a thumb from a thumb template is nearly impossible. The data is irreversible. The collection of points is simply not sufficient to reproduce a thumb, hand or face.

"A biometric is a binary representation of a unique physical attribute that you cannot reverse engineer easily," says Paul Collier, executive director of the Biometric Foundation. "And as just data, it's meaningless." A criminal wanting to invade your privacy will have more luck with your Social Security number than with any biometric data.

Plzak chose fingerprint readers because they're unobtrusive, accurate and cheap — three factors that vary among the various biometric technologies. Plzak decided against hand readers because they take up too much room on the desktop. Although iris scanning is extremely effective, it's also expensive and intrusive. A camera on the desktop makes users feel as if they're being watched. Fingerprint readers are rather small and when incorporated into a keyboard or notebook computer, they're unobtrusive. When it comes time for the full county rollout, Plzak hopes to buy fingerprint readers for as little as $35 per unit.

In an effort to get the county to bite on his pilot phase, Plzak rolled out a handful of units to the most high-profile users. "They are probably the ones that can make the decision on budget to go forward." He understands that users will need to be acclimatized to biometrics. That's why he's giving everyone a choice to log on via a secure password or thumbprint reader. Eventually he hopes to push everyone toward biometrics.

Paul Collier
Executive Director of the Biometric Foundation

Anxiously Circling

Securing access for 3,000 users in one county is tough. Coming up with a solution for 11 million people as they move across the country is much harder. Such is the task of the newly created Transportation Security Administration (TSA). The organization has been charged with establishing a uniform security system across all airports nationwide. In an effort to determine the best solution, the TSA has been requesting information and running tests at 20 airports. Some other airports are running tests independently, but most are in a holding pattern patiently waiting for the TSA's recommendations.

While many are circling trying to figure out the best course of action, others just point to the 12-year success of secure access at San Francisco International Airport (SFO). The airport significantly raised the security bar by successfully implementing a network of more than 500 dual-validation access units, of which more than 200 are used by the airport's 21,000 employees. The remainder are reserved for emergency personnel like police and firefighters.

To enter through one of SFO's secured access points, the user must swipe a card and then press his or her hand against the hand-geometry reader. The benefit, raves Mark Denari, Assistant Deputy of Airport Security at SFO is that "you're validating the card and the person." Unlike the airport's previous card-only access system, the dual validation system means a lost card becomes useless to any other user. The biometric scanner is close to flawless claims Denari. He's had limited problems during enrollment, and estimates cases of false positives run somewhere in the neighborhood of 0.01 percent.

Even with nearly perfect equipment, SFO still has had security breaches. The scanning system had no ability to force users to close the door. This loose end became a very real problem at SFO. So three years ago, during an access control

CREDIT AND SOURCE INFORMATION HERE

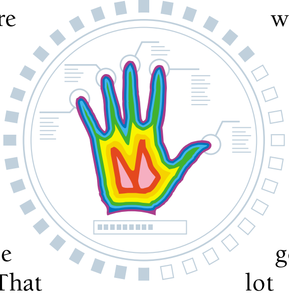
audit by the Department of Transportation, Denari began examining employee access. He noticed that about 40 percent of people who opened a door did not ensure that it closed. Reminding people to shut the door may have alleviated some of the problem, but it wouldn't have eliminated it. Denari, a former architect, thought to himself, "How can I design a solution that will engineer out the problem?"

The solution was to attach turnstile vestibules to the problematic doors. The user first swipes the card to get through the door, and then there is a full system (card and hand reader) to get through the turnstile. For those employees who need to get equipment like garbage cans through, he created a four-foot-high bypass door that could be opened only with a key that received limited distribution (see diagram). Denari maintains, "Once we facilitated that solution we've had 100 percent security in terms of controlling access. We've had no security breaches."

Tom Jewsbury
Director of Airport Operations
St. Petersburg

Know Your Passengers

If you choose to fly out of St. Petersburg-Clearwater (Fla.) International Airport in the near future, you'll find yourself undergoing a new security procedure. Since January 24, 2002, all passengers who initiate flights from St. Petersburg must pass through one of two face recognition systems. Unlike the previous examples, where biometrics authenticate known users, St. Petersburg Airport uses biometrics to identify unknown users.



At the security checkpoint, passengers stand in front of the face scanner for a picture. That picture is mapped with up to 128 unique facial points and then compared to an image database of 5,000 known terrorists and high-profile criminals. If a match occurs, the image and accompanying information appear on screen for the deputy working the station, while a similar alert is sent wirelessly to a TSA agent's PDA. A match does not denote grounds for an arrest. It only alerts agents to investigate further the subject's credentials.

People do not take face scanning lightly. During the Super Bowl and on the streets of the Ybor City neighborhood, the Tampa Bay, Fla., area had already been exposed to face recognition. In both instances, the technology was used to scan faces in a crowd. Many felt their privacy was invaded because they didn't know when and where they were being scanned. "We knew it was controversial at the time, especially actually in the Tampa Bay area. So we were very cautious going into it. We had to get a lot of people's comfort level up," says Tom Jewsbury, director of airport operations at St. Petersburg. Acceptance of the airport's biometric system depended on educating government officials and the public. Using the media, Jewsbury made it clear that what the airport was doing was different. Everyone knew when and where they were being scanned. There would be no roaming crowd scans. In addition, they reminded everyone that the system does not track subjects who do not appear in the database. If a face doesn't match, the system expunges the image immediately.

The Buy-in Challenge

Public acceptance of biometrics will still take some time. Besides the cost factor, most biometric technologies introduce new systems that must be re-engineered for humans to accept and understand. In some instances, where biometrics simply improve an already established system, the challenge is less onerous. In the case of fingerprinting, because the public was well aware of the need and value of fingerprint identification, the digital process met with little resistance.

For other more innovative and perhaps less familiar biometric technologies, the challenge of building public acceptance increases. It's not enough to prove consistently a technology's worth, with failure rates far below other comparable security systems. Public buy-in requires far more than impressive specifications and use statistics. Lacking legislative mandates or some degree of pre-existing public familiarity, the adoption of innovative biometric systems will likely continue to be slow and sporadic. ◆

CREDIT AND SOURCE INFORMATION HERE