

NEW JERSEY  
**TECH** *interactive* **NEWS**  
The Business Behind the Technology Sectors of New Jersey

A man in a dark suit, light blue shirt, and patterned tie is smiling and pointing his right index finger towards a glowing green fingerprint graphic. The graphic is a stylized representation of a fingerprint with radiating lines, appearing to be scanned or highlighted. The background is a plain, light-colored wall.

**At Your Fingertips...**  
**Biometrics Provides Secure Access**  
**to Valuable Resources**

# At Your Fingertips...

## Biometrics Provides Secure, Convenient Access to Valuable Corporate Resources

BY CHARLES "BUD" YANAK

User authentication is widely considered the weakest link in any security system. When implementing security measures for access to facilities, corporate networks and "secure" websites, organizations must strike a balance to provide a method for identifying individuals that is both secure and convenient

It's no secret that the continued increase in identity theft and account "hijacking" is evidence that ID badges and passwords, the de facto standards for establishing user identity, are easily compromised. Organizations are forced to establish and maintain procedures to help ensure that this doesn't happen. To improve password integrity, for example, organizations often adopt rules such as mandating minimum password length or requiring users to frequently change their passwords.

These extra protections, however, come at a high cost. Unless the user records each password for future reference, passwords are easily forgotten. The net result is that passwords and tokens not only provide inadequate security but are also a constant headache for users and IT staff. According to Forrester Research, each password reset request cost the average organization \$13. This does not take into account the lost productivity experienced when a user can't access needed information because he forgot his password.

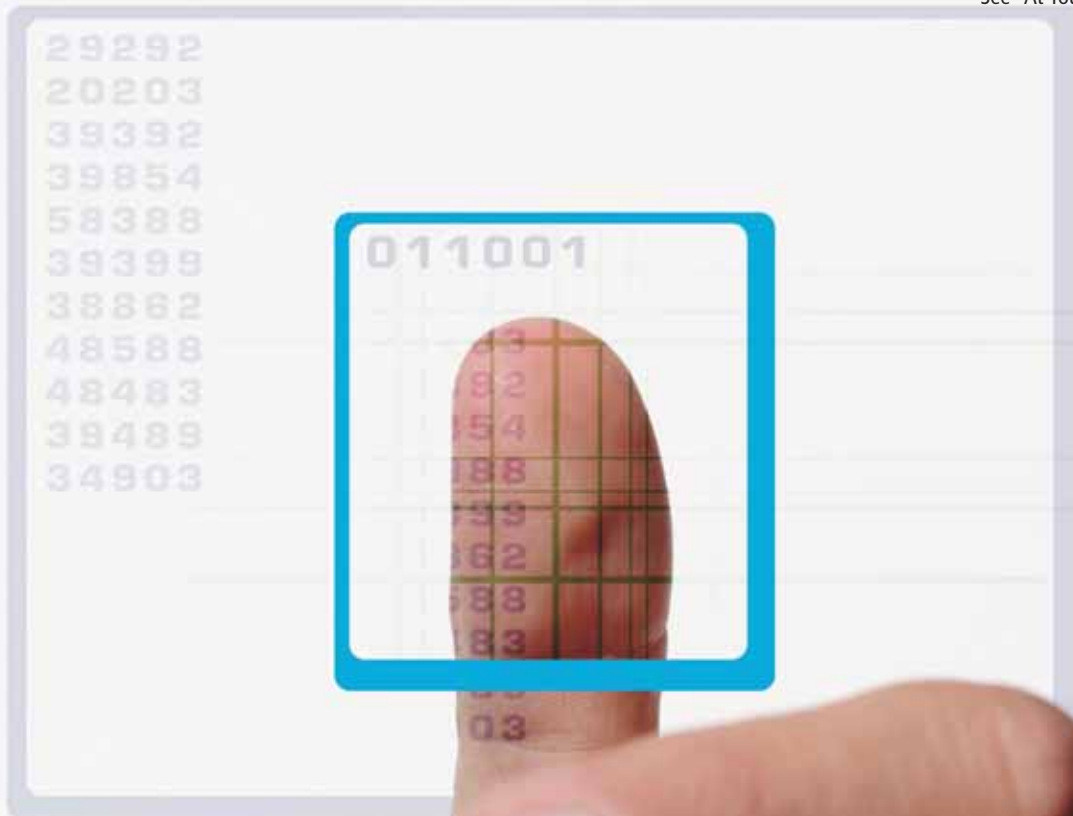
As an alternative, some organizations have deployed password-generating devices or "password tokens" to improve security. These tokens and their corresponding authentication server generate a time

synchronized pass-code that replaces the traditional password. To serve its intended purpose, the pass-code can remain valid for only a short time, and users often complain that by the time they enter the complete pass-code it has expired, forcing them to repeat the entry process. Tokens are expensive to deploy and maintain. Additionally, they are usually designed to attach to key chains and as a result, they have the same problems as keys and ID badges; they can be lost, damaged or stolen. Furthermore, these tokens, along with the user's PIN, can be shared with other people just like passwords.

Multiple studies confirmed what many network administrators have known for years: most corporate hacking and non-permitted access are actually the result of internal sharing of ID cards and passwords. Tokens are just as easily shared, so they don't really address the larger unauthorized-sharing issue endangering networks today, and any token is just as easily lost, damaged or stolen as a traditional password.

The strongest, most secure networks, including those entrusted with national security data, incorporate biometric identifiers as a key credential to establish an individual's identity. Biometrics involves the enrollment and comparison of physical characteristics, such as a fingerprint, to uniquely identify a person. Fingerprints are the most common biometric mode employed today for two reasons. First, fingerprint input devices have become widespread, affordable and easy to use. Major manufacturers such as DELL, HP and Microsoft offer a range of standard fingerprint enabled

See "At Your Fingertips," page 10



# At Your Fingertips...

continued from page 6

products such as laptops, mice and keyboards. More than 17 million laptops with built-in fingerprint readers have been sold worldwide. Second, the software for scanning and verifying fingerprints has reached a high level of maturity to accurately and quickly identify an individual in databases containing millions of people.

## Worth the Investment?

Absolutely! Biometric user identification represents a win-win for organizations. The end user no longer needs to remember passwords or carry ID tokens, and enterprise security managers can cut operating costs while at the same time improving security. Biometric solutions are being integrated into virtually every type of security application to combat identity theft and account "hijacking."

The U.S. government also sees the value that biometrics offer in improving security.

Homeland Security Presidential Directive 12 (HSPD-12) requires federal employees' and government contractors' biometric data to be captured for personal identity verification to control access to buildings and systems.

Biometrics offers organizations of any size a "Doorway to Desktop" identity alternative to establish the identity of individuals before granting access to facilities or to a corporate LANs. In order to enter the offices at one of the largest accounting firms in the United States headquartered in Philadelphia, employees and registered visitors simply place their finger on a conveniently located fingerprint reader to gain access. Consequently, employees and visitors no longer need to carry keys or ID cards and are not burdened with having to remember PINs. A single fingerprint-based solution also eliminates the need to acquire and maintain separate card access systems for facilities and password or token-based systems for systems and networks. The result is lower total costs for acquisition and maintenance.

AT&T recently outfitted stores with portable tablet computers so staff can roam the store and address the immediate needs of customers. With this mobile POS platform, the staff can now conduct transactions ranging from answering account questions to processing accessory purchases, anywhere in the store. Because these devices operate wirelessly, PCI regulations and corporate security dictated that access to these devices and the back-end retail systems be protected with authentication at a user, not device level.

Traditional authentication methods such as "One Time Password" devices proved too cumbersome to use with the mobile form factor. Additionally,

the mobile devices are shared among retail staff, so authentication is performed frequently. The IT staff of AT&T chose a fingerprint biometric solution over passwords and token alternatives because of the superior security offered and the speed and ease of use for the staff.

Consumers and system users alike acknowledge the value that biometrics offer in protecting identity. Fingerprint technology has been widely used by law enforcement agencies to verify and match fingerprints. With the proliferation of inexpensive fingerprint readers that have been integrated into devices including laptops and cell phones, user acceptance for commercial fingerprint biometric applications continues to grow.

A recent (December 2008) Unisys survey concluded that a majority of Americans are comfortable using common biometric technologies for authentication. More than 70 percent of respondents will trust banks and government agencies to ask them for biometric data for identity verification. Additionally, the survey results show fingerprints nearly tied personal passwords as the primary preferred authentication method, 73 percent to 72 percent, respectively.



## The Future is Today

"Biometric identification and authentication are coming of age and we are beginning to see deployments that will touch our everyday lives such as withdrawing money from biometrically enabled ATMs, gaining access to offices without the need for keys and replacing passwords to login to corporate networks," said Mike DePasquale, CEO of BIO-key International, a leading provider of fingerprint biometric software solutions, based in Wall. "New Jersey has been a great place to operate our business and launch some of the most advanced technology that exist for positive identification; we expect the business to grow significantly this year and beyond."

Fingerprint-based biometrics and more traditional techniques, such as passwords,

tokens or PIN-based ID cards, are not incompatible and can be used together where appropriate. Recently many network administrators have focused on multi-factor authentication (involving two or more methods of authentication) to protect high-value assets and sensitive data. Biometric authentication solutions can be easily added to provide an excellent additional factor to new or existing authentication infrastructures looking for the improved security that multi-factor authentication provides.

*Charles "Bud" Yanak is the vice president of marketing for BIO-key International, Inc. Visit [www.bio-key.com](http://www.bio-key.com) for more information.*



## BIO-key International

Not all biometric solutions are equal. With years of experience working with government agencies and public corporations, BIO-key International of Wall recognizes the balance between convenience and security. The company's patented algorithms -- which process and match the fingerprints -- capture thousands of data points from a single finger image, allowing the software to rapidly and accurately identify or authenticate a person in databases with millions of fingerprints.

With this solid foundation, BIO-key offers scalable enterprise-strength solutions, which allow application developers, system integrators and organizations to leverage their existing network infrastructure investments.

Case in Point: Parente is one of the largest accounting and consulting firms in the United States. Obviously, it is critical for Parente to be able to offer the highest level of security at its Philadelphia headquarters. When the company's management team decided to install an access control system,

it turned to a partner of BIO-key International. NextGenID Inc. put in place its system, which employs BIO-key's patented biometric matching software. Now, individuals are identified before they are granted access to Parente's facility. There's no question about who's coming and going anymore.

In order to enter Parente's offices at One Liberty Place in Philadelphia, employees and registered visitors simply place their finger on a conveniently located reader to gain access. In addition to the highest level of security, perhaps the best part is that employees and visitors no longer need to carry keys or ID cards and are not burdened with having to remember PINs.

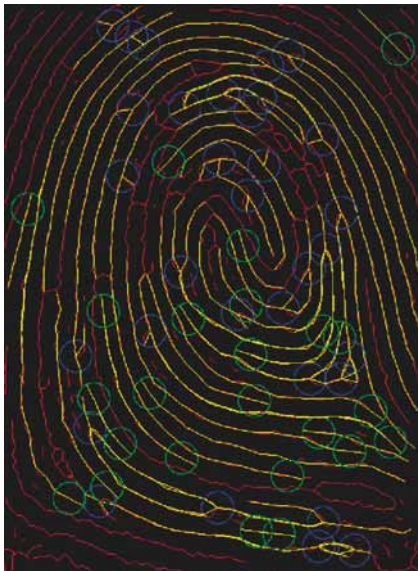
Mike DePasquale, BIO-key's president and CEO, said: "Our biometric physical and logical access solutions provide superior security without the need to carry access control cards or keys which can be reproduced, lost or stolen. Our more secure and convenient alternative to enter a facility simply relies on a person to present his finger, which a user can't forget or misplace. Virtually any organization can now

implement a 'door to desktop' identity solution based on BIO-key's superior matching algorithm to improve security, reduce cost and improve user convenience."

As in every industry, there is a wide spectrum of biometric software providers. BIO-key stands out from its competitors by being the only fingerprint biometric software company that has a mature solution that:

- is compatible with every major fingerprint reader manufacturer
- offers true "one to many" biometric identification (not just "one to one" verification)
- exceeds government and industry standards set for biometric software (BIO-key ranks first in North American based companies in overall combined average scores of all MINEX compliant algorithms tested as of January 2007).
- offers a cost effective, open architecture solution that can be easily integrated into existing database & applications

BIO-key's user authentication solutions have been implemented across the globe by health care system providers, governments, educational and financial institutions and many Fortune 500 organizations for virtually every logical and physical entry access application. BIO-key is also one of the largest providers of mobile and wireless public safety solutions in America. Over 50 law enforcement agencies in New Jersey rely on BIO-key mobile wireless solutions to deliver critical information to their officers - while at a traffic stop or other incident - on a person or vehicle directly from national, regional and local databases.



OFFSET THE ECONOMIC DOWNTURN...

### *Can effective asset lifecycle management reduce IT operational costs?*

The old sailor's pearl of wisdom, "you can't know exactly where you are going if you don't know exactly where you are" rings particularly true for IT departments in these turbulent economic times. While many companies have simply put an overall freeze on all IT projects and spending, RennerBrown is working closely with our clients to help them put a mechanism in place to accurately determine an on target baseline from which intelligent, strategic decisions can be made to optimize or upgrade existing IT resources.

That mechanism is the LANDesk Asset Lifecycle Manager. At RennerBrown, we have found, working with both our large and mid-level accounts, that comprehensive asset knowledge, accountability and control are crucial to:

- intelligent and accurate business decisions
- informed business analysis
- improved business productivity and capacity.

While in this time of frozen IT budgets it may seem counter intuitive to be asking clients to spend more money on additional technology. The fact is sometimes you need to spend more in order to save more. By knowing where your assets are and how they are being used, understanding license, acquisition, support, service and other expenses and particularly by ensuring that the right people are making the right decisions about IT gives your team control and clarity of vision. Additionally, reducing costs and enhancing overall performance allows IT to move from being a cost center to a revenue enabler.

Leveraging LANDesk's powerful Asset Lifecycle Management technology, RennerBrown is able to offer our clients the ability to substantially reduce the cost of IT operations.



**RENNERBROWN**

IF YOU WOULD LIKE TO LEARN MORE OR DISCUSS HOW RENNERBROWN CAN ASSIST IN LOWERING SUPPORT COSTS IN YOUR ENVIRONMENT PLEASE CALL US AT 1-800-276-9712 OR EMAIL BOBT@RENNERBROWN.COM