IDG .com

NETWORKWORLD® Reprint

The leader in network knowledge ■ www.networkworld.com August 21, 2006 ■ Volume 23, Number 32

Bankers giving the finger to network security

BY JOHN FONTANA

For Daren Mehl, securing billions of dollars in transactions is so easy he can do all the heavy lifting with just a finger.

Mehl, the assistant vice president of technology for United Banker's Bank (UBB) in Bloomington, Minn., found his strength in biometrics with the deployment of fingerprint readers that employees and UBB affiliates use to securely log into online resources locally and over the Internet.

The fingerprint readers, developed by DigitalPersona, anchor a multifactor authentication and single sign-on system for some 2,500 users who don't have to remember multiple passwords – just which finger to press onto the small USB-connected scanner.

In addition, UBB's system is far out in front of guidelines set forth in October 2005 by the Federal Financial Institutions Examination Council calling for Internet banking to adopt two-factor authentication by January 2007.

Long before that announcement, Mehl and UBB were perfecting and expanding their system that went live internally in 2001 and externally in 2003. They plan to further extend the fingerprint technology to help thwart phishing and secure wire transfers.

"We need to know who our customers are and so we wanted a stronger authentication system," he says. "From a security standpoint, I saw the writing on the wall with key loggers and spyware and I knew we needed a second form of authentication."

The bank picked fingerprints over security tokens because tokens can be shared and a fingerprint cannot. "We need to make sure who is sending money," Mehl says.

UBB provides that assurance and more to its customers, who just so happen to own and operate UBB, which was the first bank for bankers when it opened in 1975.

Those owners are 1,200 community banks that pool resources under UBB so they can provide their customers with services such as check cards and major loans. More than 250 shareholders with combined assets of $7.8 billion have invested in the bank, whose services let the member banks – located throughout Minnesota, the Dakotas, Nebraska, Montana, Wyoming and Iowa – operate like the heavyweights of the banking industry.

And Mehl and his staff operate as the security heavyweights among the 20 or so banker's banks that operate throughout the country, having helped three other community-bank-supported co-ops reproduce UBB's fingerprint infrastructure.

For UBB's internal users, the fingerprint readers serve as a single sign-on to applications and Web sites. For member banks – UBB's customers – the fingerprint reader fronts access to online accounts and a transaction system used to move money.

It all works from a Windows-based back end comprised of Active Directory and Windows Server 2003, and complemented by backup, disaster recovery and a DigitalPersona server to handle online registration and fingerprint data exchange.

For internal users, the system is managed locally and has relieved Mehl and his staff of the headache of password resets.

"We have about six or seven internal systems with passwords that are set to expire every 90 days and we have 80 users," Mehl says. "[Before the fingerprint reader] we probably had to reset two or three passwords a day in any given system." Now, he says, they reset a password "every once in a while."

With biometrics, internal users register the user names and passwords they have for each system. The data is stored in an encrypted file and retrieved only when the user wants to log on and only when their fingerprint is a match authorizing retrieval.

UBB customers who access UBB systems over the Internet must first register their fingerprint in the system. The bank sends them one free fingerprint scanner to get started and offers any technical support needed, although Mehl says UBB has not had to do any training, just a bit of handholding for the three-step installation process.

Also important, he says, is that the fingerprint image is never recorded anywhere.

"At no time does the PC see the actual fingerprint; it is always encrypted," Mehl says. "The scanner looks at minutia points and turns it into a mathematical number that is like 600 digits."

The DigitalPersona Online Server, which runs on Microsoft's SQL Server and Internet Information Server, negotiates an exchange of the fingerprint data via the DigitalPersona software installed on a PC. The exchange is secured by a private key (the fingerprint data) / public key (the UBB site) infrastructure.

Mehl says UBB adapted the fingerprint system in 2003 for use with its reporting system, which gives account and other information, and in 2005 for its transaction system, but logon to the two systems remains separate for security reasons.

Now Mehl is turning the fingerprint scanner into a security token that can add another layer to authentication.

The newest DigitalPersona scanners include an internal serial number that is communicated to the DigitalPersona Online server and Mehl is now storing those numbers so he can match them to specific fingerprint readers at each logon.

"So we have the user name, the fingerprint, the physical token and we block by IP address so that gives us four authentication mechanisms,"he says.

Next year, Mehl plans to add another that will let customers authenticate UBB to help defend them against phishing attacks.

Mehl says he has not totaled the costs or quantified the returns but like a true banker says, "I wouldn't call it expensive, I would call it an investment."

Mehl has even linked the fingerprint reader into the PC's desktop screensaver so only the proper user can unlock the PC. ■