BIOMETRIC AUTHENTICATION SYSTEMS FOR CREDIT CARDS COULD PUT IDENTITY THIEVES OUT OF BUSINESS

A TOUCH OF MONEY

HE STOLE THE IDENTITIES of the world's rich and famous—Paul Allen, Oprah Winfrey, Steven Spielberg, Warren Buffett, and Larry Ellison, to name a few. Until the New York City police busted 32-year-old Abraham Abdallah, it seemed that a diabolically gifted hacker, not a busboy at a Brooklyn restaurant, had masterminded this multimillion-dollar caper.

However, a tattered copy of a *Forbes* magazine featuring America's 400 richest people found in Abdallah's possession—along with 800 credit cards—exposed the thief's simple modus operandi. Here were his targets, listed in order of their net worth, some with Social Security numbers and credit card information scrawled right next to their names. Investigators soon discovered that Abdallah had obtained most of this information from the Internet, as well as from credit bureaus Equifax, Experian, and TransUnion, by sending queries on the forged letterhead of several top investment banks.

With birth dates, addresses, and Social Security and credit card numbers in hand, Abdallah would use a computer at a public library to order merchandise online, withdraw money from brokerage accounts, and apply for credit cards in other people's names. Things started to unravel when he tried to transfer US $10 million from the Merrill Lynch account of software entrepreneur Thomas Siebel. Someone at Merrill Lynch noticed that the same two Yahoo e-mail addresses, both Abdallah's, had been used in connection with five other clients. Soon after, on 19 March 2001, two New York City detectives wrestled Abdallah out of his car, ending one of the most sensational identity theft sprees in history.

JOHN WEBER

BY ANIL K. JAIN & SHARATHCHANDRA PANKANTI

POSITION
MATCH
$1

SCANNERS GALORE: Biometric ID systems are proliferating everywhere except in credit cards. A Pay By Touch fingerprint scanner for buying groceries [top]; an ATM with a Fujitsu PalmSecure palm vein scanner [middle]; a fingerprint sensor from AuthenTec in an LG Electronics phone.

Catching ID thieves is like spearfishing during a salmon run: skewering one big fish barely registers when the vast majority just keep on going. According to data from the Aberdeen Group, Boston, the cumulative losses suffered by tens of millions of individuals and businesses worldwide registered at an estimated $221 billion in 2003. Aberdeen, which assumed an enormous 300 percent compound annual growth rate, projected that losses would rise to an almost unfathomable $2 trillion in 2005. More recent numbers from Javelin Strategy and Research, based in Pleasanton, Calif., indicate a much lower growth rate, at least in the United States, where total losses rose from about $48 billion in 2003 to $56.6 billion in 2005.

Clearly, it is far too easy to steal personal information these days—especially credit card numbers, which are involved in more than 67 percent of identity thefts, according to a U.S. Federal Trade Commission study. It's also relatively easy to fake someone's signature or guess a password; thieves can often just look at the back of an ATM card, where some 30 percent of people actually write down their personal identification number (PIN) and give the thief all that's needed to raid the account. But what if we all had to present our fingers or eyes to a scanner built into our credit cards to authenticate our identities before completing a transaction? Faking fingerprints or iris scans would prove challenging to even the most technologically sophisticated identity thief.

The sensors, processors, and software needed to make secure credit cards that authenticate users on the basis of their physical, or biometric, attributes are already on the market. But so far, the credit card industry hasn't seen fit to integrate even basic fingerprint-sensing technology with their enormous IT systems. Concerned about biometric system performance, customer acceptance, and the cost of making changes to their existing infrastructure, the credit card issuers apparently would rather go on eating an expense equal to 0.25 percent of Internet transaction revenues and the 0.08 percent of off-line revenues that now come from stolen credit card numbers.

Indeed, only a few companies worldwide have even experimented with biometric credit cards. The best known is the Bank of Tokyo–Mitsubishi. Since 2004, it has issued Visa cards embedded with chips that identify a customer according to vein patterns in the palm. All of the bank's ATMs have palm scanners that match the imaged vein patterns to a digitized copy of the customer's vein patterns—called a biometric template—that is stored in the card. But because merchants lack the requisite palm scanners to go with this technology, customers still sign receipts or enter PINs when making purchases with the card.

All biometric systems recognize patterns, such as the veins in your palms, the texture of your iris, or the minutiae of your fingerprints. As researchers who have investigated and engineered numerous biometric devices, we want to propose the broad outlines of a new authentication system for credit cards, based on biometric sensors that could dramatically curtail identity theft. Our proposed system uses fingerprint sensors, though other biometric technologies, either alone or in combination, could be incorporated. The system could be economical, protect privacy, and guarantee the validity of all kinds of credit card transactions, including ones that take place at a store, over the telephone, or with an Internet-based retailer. By preventing identity thieves from entering the transaction loop, credit card companies could quickly recoup their infrastructure investments and save businesses, consumers, and themselves billions of dollars every year.

If credit card issuers don't act soon, customers, many of whom are becoming increasingly comfortable with biometric technologies, might just force the issue. In the United States, millions of people at hundreds of supermarkets have already given the

FROM TOP: PAY BY TOUCH; FUJITSU LTD.; AUTHENTEC

thumbs-up to services offered by BioPay LLC, Herndon, Va., and Pay By Touch, San Francisco, which let shoppers pay for their groceries by pressing a finger on a sensor mounted near the cash register—no card necessary. Millions more, mostly in Asia, have fingerprint sensors built into their cellphones to act as locks and into their laptops to replace text-based log-ins. All of this activity translates to 29 percent annual growth for a worldwide biometrics market that's expected to reach $3.4 billion in 2007, according to Research and Consultancy Outsourcing Services, a market research organization based in New Delhi, India. Finger-scanning technology made by companies like Atmel, AuthenTec, Digital Persona, Fujitsu, and Identix will account for almost 60 percent of the total market, the organization estimates. And that market will greatly expand if and when credit card companies get serious about combating ID theft [see photos, "Scanners Galore"].

CURRENT CREDIT CARD authentication systems validate anyone—including impostors—who can reproduce the exclusive possessions or knowledge of legitimate cardholders. Presenting a physical card at a cash register proves only that you have a credit card in your possession, not that you are who the card says you are. Similarly, passwords or PINs do not authenticate your identity but rather your knowledge. Most passwords or PINs can be guessed with just a little information: an address, license plate number, birth date, or pet's name. Patient thieves can and do take pieces of information gleaned from the Internet or from mail found in the trash and eventually associate enough bits to bring a victim to financial grief.

Besides trawling the Internet and diving into dumpsters for personal data, thieves exploit people through various cons known collectively as social engineering. A smooth-talking grifter can sometimes get a customer service representative to part with a PIN or reveal other things about an account, such as a mailing address or a phone number. The bank makes it easier for thieves if its authentication protocol is riddled with exceptions. For instance, if you don't know the PIN, you might be able to provide a mailing address, mother's maiden name, phone number, or Social Security number to get access to—or at least information about—a particular account. Sometimes those bits of data can be harvested from other sources.

Furthermore, customer service representatives and their managers can usually override authentication procedures when they deem it necessary. A caffeine-addled agent working a double shift may be only too eager to use her override privileges to let you—or your would-be doppelgänger—make a purchase.

To ensure truly secure credit card transactions, we need to minimize this kind of human intervention in the authentication process. Such a major transition will come at a cost that credit card companies have so far declined to pay. They are particularly worried about the cost of transmitting and receiving biometric information between point-of-sale terminals and the credit card payment system. They also fret that some customers, anxious about having their biometric information floating around cyberspace, might not adopt the cards. To address these concerns, we offer an outline for a self-contained smart-card system that we believe could be implemented within the next few years.

Here's how it would work. When activating your new card, you would load an image of your fingerprint onto the card. To do this, you would press your finger against a sensor in the card—a silicon chip containing an array of microcapacitor plates. (In large quantities, these fingerprint-sensing chips cost only about $5 each.) The surface of the skin serves as a second layer of plates for each microcapacitor, and the air gap acts as the dielectric medium. A small electrical charge is created between the finger surface and the capacitor plates in the chip. The magnitude of the charge depends on the distance between the skin surface and the plates. Because the ridges in the fingerprint pattern are closer to the silicon chip than the valleys, ridges and valleys result in different capacitance values across the matrix of plates. The capacitance values of different plates are measured and converted into pixel intensities to form a digital image of the fingerprint [see diagram, "Fingerprint Matching"].

Next, a microprocessor in the smart card extracts a few specific details, called minutiae, from the digital image of the fingerprint. Minutiae include locations where the ridges end abruptly and locations where two or more ridges merge, or a single ridge branches out into two or more ridges. Typically, in a live-scan fingerprint image of good quality, there are 20 to 70 minutiae; the actual number depends on the size of the sensor surface and the placement of the finger on the sensor. The minutiae information is encrypted and stored, along with the cardholder's identifying information, as a template in the smart card's flash memory.

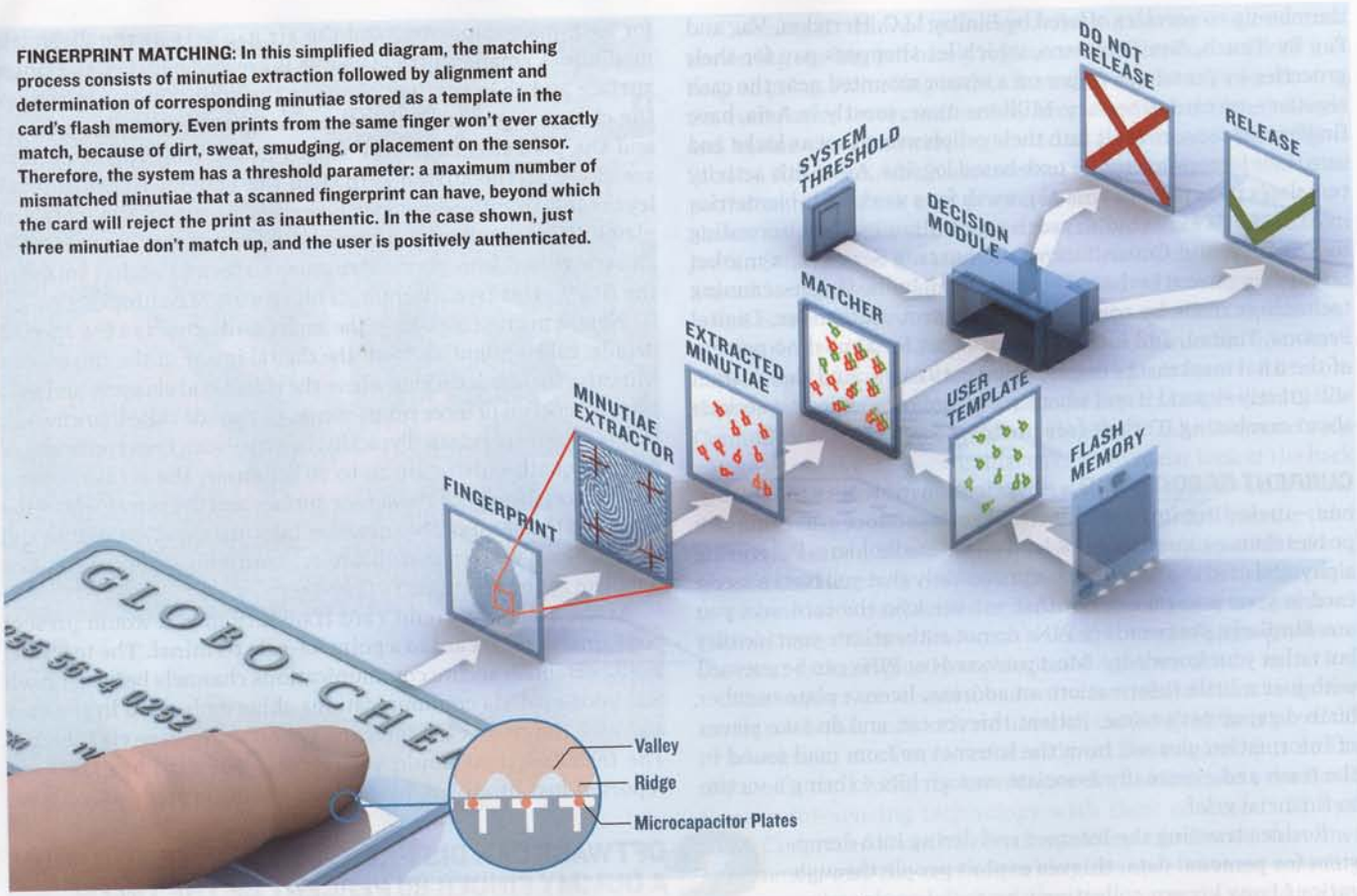
At the start of a credit card transaction, you would present your smart credit card to a point-of-sale terminal. The terminal would establish secure communications channels between itself and your card via communications chips embedded in the card and with the credit card company's central database via Ethernet. The terminal then would verify that your card has not been reported lost or stolen, by exchanging encrypted information with the card in a predetermined sequence and checking its responses against the credit card database.

SOFTWARE CAN DISTINGUISH A REAL FINGER FROM A DUMMY FINGER 85 PERCENT OF THE TIME—ENOUGH TO MAKE YOUR AVERAGE IDENTITY THIEF THINK TWICE BEFORE FASHIONING A FAKE

Next, you would touch your credit card's fingerprint sensor pad. The matcher, a software program running on the card's microprocessor, would compare the signals from the sensor to the biometric template stored in the card's memory. The matcher would determine the number of corresponding minutiae and calculate a fingerprint similarity result, known as a matching score. Even in ideal situations, not all minutiae from the input and template prints taken from the same finger will match. So the matcher uses what's called a threshold parameter to decide whether a given pair of feature sets belong to the same finger or not. If there's a match, the card sends a digital signature and a time stamp to the point-of-sale terminal. The entire matching process could take less than a second, after which the card is accepted or rejected.

The point-of-sale terminal sends both the vendor information and your account information to the credit card company's transaction-processing system. Your private biometric information remains safely on the card, which ideally never leaves your possession.

But say your card is lost or stolen. First of all, it is unlikely that a thief could recover your fingerprint data, because it is encrypted and stored on a flash memory chip that very, very few thieves would have the resources to access and decrypt. Nevertheless, suppose that an especially industrious, and perhaps unusually attractive, operator does get hold of the fingerprint of your right index finger—say, off a cocktail glass at a hotel bar where you really should not have been drinking. Then this industrious thief manages to fashion a latex glove molded in



FINGERPRINT MATCHING: In this simplified diagram, the matching process consists of minutiae extraction followed by alignment and determination of corresponding minutiae stored as a template in the card's flash memory. Even prints from the same finger won't ever exactly match, because of dirt, sweat, smudging, or placement on the sensor. Therefore, the system has a threshold parameter: a maximum number of mismatched minutiae that a scanned fingerprint can have, beyond which the card will reject the print as inauthentic. In the case shown, just three minutiae don't match up, and the user is positively authenticated.

a slab of gelatin containing a nearly flawless print of your right index finger, painstakingly transferred from the cocktail glass.

Even such an effort would fail, thanks to new applications that test the vitality of the biometric signal. One identifies sweat pores, which are just 0.1 millimeter across, in the ridges using high-resolution fingerprint sensors. We could also detect spoofs by measuring the conduction properties of the finger using electric field sensors from AuthenTec Inc., of Melbourne, Fla. Software-based spoof detectors aren't far behind. One of us (Jain) is currently leading an effort at Michigan State University, in East Lansing, in which researchers are differentiating the way a live finger deforms the surface of a sensor from the way a dummy finger does. With software that applies the deformation parameters to live scans, we can automatically distinguish between a real and a dummy finger 85 percent of the time—enough to make your average identity thief think twice before fashioning a fake finger.

NO SYSTEM IS PERFECT, of course, including the one we propose. Any biometric system is prone to two basic types of errors: a false positive and a false negative. In a false positive, the system incorrectly declares a successful match between, in our case, the fingerprint of an impostor and that of the legitimate cardholder—in other words, a thief manages to pass himself off as you and gains access to your accounts. In the case of a false negative, on the other hand, the system fails to make a match between your fingerprint and your stored template—the system doesn't recognize you and therefore denies you access to your own account.

According to a 2003 National Institute of Standards and Technology report, a stand-alone fingerprint system might achieve a 1 percent false-positive rate and a corresponding false-negative rate of 0.1 percent. So if such a system were used in conjunction with the existing means used to secure credit cards (such as PINs and signatures), the system's security could be 100 times as effective, while at the same time incorrectly rejecting just one more transaction per every 1000 than are rejected today. We think that credit card users will tolerate this slight additional inconvenience in exchange for far more effective security.

How much they will pay for that additional peace of mind is unknown. But certainly, it need not be expensive. Costs are declining for all of the major smart-card components, including flash memory, microprocessors, communications chips, and fingerprint sensors. Indeed, the basic physical card already exists, albeit in the form of a keychain fob from Privaris Inc., in Fairfax, Va. The company's wireless dongle has all the hardware components mentioned here, and it is likely that sufficient sales volume could cut the retail price of the device from $200 to $20 in a couple of years. The dongle uses fingerprint-based user authentication to release data, such as an access code, needed to perform a transaction. The fingerprint is sensed, stored, and processed only on the device and is never released, so as to protect the user's privacy. It would be possible to cut costs further by harnessing the mass-market biometric sensors and computing power available in today's cellphones and programming them with data-matching software and digital certificates.

A version of the system designed to protect Internet shoppers might be even easier to implement, and less expensive, too. When mulling the costs and benefits of biometric credit cards, card issuers might well decide to first deploy biometric authentication systems for Internet transactions, which is where ID thieves cause them the most pain. A number of approaches could work, but here's a simple one that adapts some of the basic concepts from our proposed smart-card system.

To begin with, you'd need a PC equipped with a biometric sensing device such as a fingerprint sensor, a camera for iris scans, or a

BRYAN CHRISTIE DESIGN

microphone for taking a voice signature. Next, you'd need to enroll in your credit card company's secure e-commerce system. You would first download and install a biometric credit card protocol plug-in for your Web browser. The plug-in, certified by the credit card company, would enable the computer to identify its sensor peripherals so that biometric information registered during the enrollment process could be traced back to specific sensors on a specific PC. After the sensor scanned your fingerprints, you would have to answer some of the old authentication questions—such as your Social Security number, mother's maiden name, or PIN. Once the system authenticated you, the biometric information would be officially certified as valid by the credit card company and stored as an encrypted template on your PC's hard drive.

During your initial purchase after enrollment, perhaps buying a nice shirt from your favorite online retailer, you would go through a conventional authentication procedure that would prompt you to touch your PC's finger scanner. The credit card protocol plug-in would then function as a matcher and would compare the live biometric scan with the encrypted, certified template on the hard drive. If there were a match, your PC would send a certified digital signature to the credit card company, which would release funds to the retailer, and your shirt would be on its way. Accepting the charge for the shirt on the next bill by paying for it would confirm to the card issuer that you are the person who enrolled the fingerprints stored on the PC. From then on, each time you made an online purchase, you would touch the fingerprint sensor, the plug-in would confirm your identity, and your PC would send the digital signature to your credit card company, authorizing it to release funds to the vendor.

If someone else tried to use his fingerprints on your machine, the plug-in would recognize that the live scan didn't match the stored template and would reject the attempted purchase. If someone stole your credit card number, enrolled her own fingerprints on her own PC, and went on an online shopping spree, you would dispute the charges on your next bill and the credit card issuer would have to investigate.

BIOMETRIC AUTHENTICATION SYSTEMS based on available technology would be a major improvement over conventional authentication techniques. If widely implemented, such systems could put thousands of ID thieves out of business and spare countless individuals the nightmare of trying to get their good names and credit back. Though the technology to implement these systems already exists, ongoing research efforts aimed at improving the performance of biometric systems in general and sensors in particular will make them even more reliable, robust, and convenient.

Remember, no practical biometric system makes perfect match decisions all the time. As a result, thieves occasionally succeed in being positively identified as people they are not, while legitimate users are sometimes incorrectly rejected. That's because two different samples of the same biometric identifier are never identical. There are two main reasons for this.

First, the sensed biometric data might be noisy or distorted—a cut on your finger leaves a fingerprint with a scar, or a cold alters your voice, for example. Noisy data can also result from improperly maintained sensors—say, from dirt on a fingerprint sensor—or from unfavorable sensing conditions, such as poor focus on a user's iris in a recognition system.

Second, the biometric data acquired during authentication may be very different from the data used to generate the template during enrollment. During authentication, a user might touch a sensor incorrectly or blink an eye during iris capture.

Some errors might be avoided by using improved sensors. For instance, optical sensors capture fingerprint details better than capacitive fingerprint sensors and are as much as four times as accurate. Even more accurate than conventional optical sensors, the new multispectral sensor from Lumidigm Inc., in Albuquerque, N.M., distinguishes structures in living skin according to the light-absorbing and -scattering properties of different layers. By illuminating the finger surface with light of different wavelengths, the Lumidigm sensor captures an especially detailed image of the fingerprint pattern just below the skin surface to do a better job of taking prints from dry, wet, or dirty fingers. Such sensors are already being used at Walt Disney World, in Lake Buena Vista, Fla., to admit paid visitors to the park.

Unfortunately, this kind of optical sensor cannot be easily or cheaply manufactured in a form small enough to fit on handheld gadgets or smart cards. We believe, though, that system manufacturers will push the makers of capacitive sensor technology and those who develop data-matching algorithms to close the performance gap with these more costly optical sensors while keeping prices low.

Systems based on multiple biometric traits could achieve very low error rates, but here, too, costs will be a concern. These multimodal biometric systems also make spoofing more difficult, because an impostor must simultaneously fake several biometric traits of a legitimate user. Further, by asking the user to present a random subset of two or more biometric traits—say, right iris and left index finger, in that order—the system can ensure that a live user is indeed present. Of course, that's more burdensome for the legitimate user, as well.

We are optimistic that multidisciplinary research teams in both industry and academia can find the right blend of technologies to create practical biometric applications and integrate them into large systems without introducing additional vulnerabilities. The health of the world economy, not to mention our collective peace of mind, may well depend on their efforts. ■

ABOUT THE AUTHORS

ANIL K. JAIN is a University Distinguished Professor in the departments of computer science and engineering, electrical and computer engineering, and probability and statistics at Michigan State University, in East Lansing. An IEEE Fellow, he is a coauthor of the *Handbook of Multibiometrics*, which was published this spring by Springer.

SHARATHCHANDRA PANKANTI joined IBM's Thomas J. Watson Research Center, in Yorktown Heights, N.Y., as a research staff member in 1996. Currently, he is developing general-purpose object-recognition systems. He has coedited a comprehensive book on biometrics, *Biometrics: Personal Identification in Networked Society* (Springer, 1999), and coauthored *Guide to Biometrics* (Springer, 2004).

TO PROBE FURTHER

For more information on social engineering techniques, see Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Wiley, 2002).

To learn how to fool fingerprint scanners, see "Impact of Artificial Gummy Fingers on Fingerprint Systems," by T. Matsumoto et al., in "Optical Security and Counterfeit Deterrence Techniques IV," *Proceedings of SPIE* (International Society for Optical Engineering), Vol. 4677, 2002, pp. 275–89.

A more in-depth look at the authors' work is available in "Biometrics: A Grand Challenge," by A.K. Jain, S. Pankanti, et al., in *Proceedings of the 17th International Conference on Pattern Recognition*, Vol. II, August 2004, pp. 935–42.