INTERNATIONAL BIOMETRICS & IDENTIFICATION ASSOCIATION

ID News Track

IBIA is pleased to provide ID News Track to its members. This daily service is prepared by Carroll & LaDier, PLLC.

Reports from connect:ID

New markets, new technologies – a new horizon

This is an exciting time for the biometrics industry. While traditional defense and law enforcement markets are under pressure because of concern about government spending, opportunities are growing in new sectors like banking and healthcare — and in emerging markets like Latin America and Africa.

Driving these new opportunities: smart phone ubiquity and a new generation of mobile biometric technologies.

Any smart phone with a camera is already equipped to collect at least two biometrics — voice and facial — said Terry Hartmann, vice president for security solutions and industry applications at Unisys Corp.

“It’s all already in your pocket,” said Mr. Hartmann.

“Your identity will be in the cloud, your phone is the lock, you are the key,” he summed up.

Voice + face = security

A camera-equipped smart phone can capture live video and audio of the user speaking, enabling combined voice and facial biometric checks, said Alexey Khitrov, president of SpeechPro.

Because a static facial biometric might be spoofed with a photo and a voice print with a recording, combining voice and face in this manner also helps mitigate spoofing, he said.

Voice and face are “the two biometric modalities that in our view best complement each other” in this context, he said.

Because smart phones already house secure chips from their network providers, they can also be used like secure smart cards, said Neville Pattinson, senior vice president of Gemalto.

He described how a “derived credential, a copy of the original credential in a form which can be incorporated into a mobile device,” could be used to make a smart phone an effective substitute for a smart card.

And if a smart phone can replace a smart card, why can’t it replace all those other credentials we use too?, asked Jay Meier, vice president of corporate development for BIO-key.

“The credentials that we’ve traditionally used are weak,” he said, calling a credit card “basically just a number on a piece of plastic.”

“All these credentials are becoming digitized,” he said, “As you travel through the digital world, we have to be able to ensure that you are the person allowed to access the privileges associated with those credentials.”

The key, he said, was the mobile device. “The [smart] phone will be used to administer those credentials, it will be your wallet.”

Mobile identity = mobile security

Other speakers agreed.

“I’m going to know I’ve lost this,” said Mr. Hartmann, holding up his phone, “before I know I’ve lost my credit card.”

And unlike a wallet or a credit card, a smart phone that gets stolen, if secured with biometric technology, cannot be used by the thief.

"The key to mobile security is mobile identity," said Mr. Hartmann.

Mr. Hartmann's thesis in a nutshell: Passwords don't work — he called them an "anachronism."

And challenge/response or "security" questions offer a very limited enhancement in an age where a quick social media search can often reveal a mother's maiden name or other security information.

Even two-factor authentication, which Mr. Hartmann acknowledged would stop the majority of current data breaches (four in five, by one count), is only turning a straw house into a wooden one, he said.

Is the password dead?

Two-factor authentication also tends to encounter consumer resistance, a theme that was highlighted by presenter Jeremy Grant, who heads President Obama's National Strategy for Trusted Identities in Cyberspace (NSTIC).

Mr. Grant cited poll data showing that nearly half of all Americans "would rather scrub their toilet than establish and maintain an online account" using a login ID and password.

"The password is not dead," said Mr. Grant, "But it needs to be shot, and quickly."

Mr. Hartmann's firing squad, his stone house: multi-factor authentication, including biometrics; and a risk-based rather than binary approach to identity management.

Many financial institutions already take a risk-based approach, requiring additional identity checks for larger transactions, according to Brett Beranek of Nuance communications.

In his presentation, Mr. Beranek said banks and other financial institutions were increasingly waking up to the possibilities of voice biometrics, or VB — in large part because their customers preferred it.

"When you give consumers a choice, 90 percent of them express a preference for VB as a biometric authenticator," he said, a preference which applied across generations and other demographic divides.

A 90 percent solution

The fact that an individual's voice might change over time was not a problem. "If we can hear someone speak at least once a year we can adjust their voiceprint," he said.

Indeed, the fact that voice was "not a static biometric" enabled it to impart "a richness to convenience and security," Mr. Beranek said.

"One of the key issues for us is user acceptance," he explained afterwards. "A lot of banks have had deployments [of biometric technology] which haven't worked well in terms of customer experience" and have made them chary of introducing any technologies that might encounter user resistance.

"The sales process needs to have an education step," he said, adding that voice biometrics had finally arrived. "Fingerprints had a 50-year head start."

Unlike fingerprints, voice biometrics can easily be made part of an existing customer experience on the telephone.

"We see VB as having the highest customer acceptance rates," in part because it could be so unobtrusive.

"In passive VB, you are not asking the user to say anything in particular … There's no enrollment," he explained.

Unlocking what?

Complicating the mobile authentication issue is what Mr. Pattinson called "a fragmented environment for security."

"Consumers enroll on multiple devices … and their devices have multiple service providers," said Mr. Meier.

Raising the question: Where and how do you do the authentication?

For the fingerprint-lockable Galaxy S5, Samsung chose a solution architecture that verifies identity on the phone itself, via a software client. That means the user's biometric template — in this case an image captured by the special fingerprint reader built-in to the screen — stays on the phone itself.

That's an approach that pleases privacy mavens, and it mirrors the one built into new security standards being developed by the Fast IDentity Online coalition, or FIDO.

FIDO, which includes some of the world's largest Internet, e-commerce and now financial services companies aims to "move beyond passwords" by promoting standards that enable multi-factor authentication — including biometrics like those used on the S5, the first FIDO deployment.

Last month, FIDO published its first standards, and founding coalition member PayPal announced the Galaxy S5 partnership with Samsung.

"Where and how you do the authentication is going to vary for different applications," said Tovah LaDier, of IBIA. "For a national security mission, where you might need a watchlist check, obviously you are not going to do that on the device itself.

"For point of sale applications, for smaller financial transactions, there are different requirements," she said.

Emerging markets, faster adoption

Whatever solutions architecture they adopt, banks are increasingly relying on biometrics, especially in emerging markets, where policing of identity fraud or transnational cybercrime tends to be less effective.

The adoption of customer-facing biometrics "is happening much more, much faster, in emerging markets," Vance Bjorn, chief technology officer of DigitalPersona told IBIA.

"In countries where the information and financial infrastructure is underdeveloped, there are far fewer options for secure identity" for both banks and their customers, Mr. Bjorn noted.

Without a FICO score or the huge credit reporting infrastructure that supports it; without a secure identity document like a U.S. driver's license, biometrics becomes a much more attractive option.

Mexico's Banco Azteca, which has used Digital Persona fingerprint technology since 2006, currently has almost 20 million customers enrolled and processes up to a million transactions a day, Mr. Bjorn said.

With a fingerprint reader they get from the bank, the company's website says, customers can also make biometrically secure online transactions.

"Mexico is way ahead of us" in the United States when it comes to the adoption of biometrics, especially customer-facing, Lumidigm Vice President Greg Sarrail told IBIA.

Benefits are the key

One of the beneficiaries of that forward-leaning adoption is Ingressio, a Mexico-based biometric software company that specializes in access controls and time-and-attendance solutions — authenticating punching in and punching out with fingerprints, for example.

"For businesses in Mexico, these kinds of time and attendance issues, that efficiency, they are big issues for us," Humberto Lopez Gallegos, Ingressio's director general told IBIA.

And not just in Mexico. DigitalPersona's time-and-attendance solutions are used by fast food chains in the United States, Mr Bjorn said.

"It puts an end to buddy-punching," shift-swapping and other kinds of attendance abuse, he said. And biometric logins at point-of-sale reduce register leakage for retail enterprises, too.

In Mexico, the federal government is currently enrolling beneficiaries of its universal healthcare plan, Seguro Popular, in a new biometric database, according to conference presenter Alan Gelb.

"Biometric credentials are an enabler," said Mr. Sarrail; and when they are the key to accessing benefits like free healthcare, an important line is crossed in terms of public acceptance.

Mr. Sarrail noted how the surviving leaders of the anti-apartheid struggle like retired Archbishop Desmond Tutu had promoted the South African government's launch last year of a new biometric citizen's ID card.

The card, which was rolled out first for the "Mandela generation" of older South Africans, is the key to a next-generation civic and immigration ID system being laid down by the government in Pretoria.

"They see it as an enabler, because it strips away all those extraneous elements" of identity, like race class and age, Mr. Sarrail said; while protecting against identity theft and benefit fraud.

"Cultural attitudes vary," he acknowledged. But in healthcare, even where cultural attitudes cut against biometrics, there are opportunities "driven by regulation."

In the United States, for instance, new DEA and state rules on electronic prescriptions for certain controlled drugs require two-factor authentication, Mr. Sarrail said.

The regulations allow for several different modalities of authentication.

"Ease of use, that's where we're going to get some traction" for biometric technology, he said.