| Weather | Traffic | Contact Us

Gazette.Net
Maryland Community News Online

Follow us:

Montgomery Prince George's Frederick Sports Business Politics Entertainment

Communities▾ School Life▾ Classifieds▾ GazetteBuyandSell Calendars

COMMENTS (0)

Friday, February 24, 2012

Share E-mail Comment Print

In Maryland, biometrics' eye on an elusive prize

Industry tries to connect with cybersecurity and a growing global market

by Lindsey Robbins, Staff Writer

Fingerprints, voices, facial appearances, retinas and even the distance between one's fingers: All of these reveal a person's true identity and all are part of an industry projected to reach $11 billion worldwide by 2017.

In Maryland, Gov. Martin O'Malley (D) had been making a major push to bolster the state's dominance in the cybersecurity sector. But companies engaging in biometrics — the identification and verification via biological and even behavioral traits — continue to labor outside of this focus.

Biometrics "offer security and convenience," said M. Paul Collier, president and partner at Identification Technology Partners. The Gaithersburg company provides policy, low-level engineering and analysis services regarding biometrics, advanced credentialing and forensics.

Douglas Kozlay, CEO and president of Biometric Associates in Timonium, said biometrics and cybersecurity could complement each other, with fingerprint analysis used for access control and financial transactions, while cyber-cryptographic technology and cloud technology could be used to protect the information being accessed. Biometric Associates has a patent on this fingerprint security for Internet use.

Dan Gross/The Gazette M. Paul Collier (left), president and partner of Identification Technology Partners of Gaithersburg, holds a mobile personal identity verification biometric reader, which can scan an ID card, read a fingerprint and take a photograph. At right is Thomas Baker, executive vice president and partner.

More News

“Cybersecurity is not easy to use if you have to remember all those keys and passwords,” he said.

Biometric Associates employs 2,000 and provides fingerprint analysis to keep track of people receiving government money in rural areas outside the U.S. and keep track of children in those areas.

“It’s not where I expected to be in biometrics a few years ago,” Kozlay acknowledged.

His company also produces a half-inch finger-swipe device that can hang around a user’s neck to manage time shifts for off-site workers in other companies.

Biometric Associates manufactures much of its products in Maryland, and Kozlay said there is a growing trend in the state to help its manufacturing sector.

“People like to know it’s being done locally and it doesn’t cost much to do it in the U.S. rather than outsource,” he said.

He added that his company is interested in biometric technology to analyze eye irises, but there is not yet a large enough market. Although more accurate than fingerprints, iris technology tends to be more expensive, Kozlay said.

'A tool of enhanced cybersecurity'

“We see biometrics as a tool of enhanced cybersecurity,” said John Mears, director of biometrics and identity management for Lockheed Martin Information Systems & Global Solutions in Rockville. “One of the keys to cybersecurity is knowing who is accessing and what they’re accessing.”

Vote to change state’s public defender law postponed to Monday

Frederick teachers could be furloughed

Man arrested at Prince George’s mall after crowds gather to purchase newly released Nikes

Advocates hope to repeal death penalty this session

In Montgomery, residents protest Secure Communities

BIOMETRICs 101

Face: Recognition based on facial characteristics such as tattoos, marks, scars and other visuals.
Associated with identification cards.

Fingerprint: Recognition based on differing patterns on the prints of fingers.
Associated with criminal records, background checks and visas.

Gait: Using manner of walking to determine a person's intent.
Associated with security screening, potentially at airports and heavily populated venues.

Hand geometry: Recognition based on hand characteristics such as the size of the palm, length and width of fingers, and distance between the knuckles.
Associated with security verification.

Iris: Recognition based on characteristics of the iris.
Associated with security verification.

Keystroke dynamics: Recognition based on the timing and manner of person's typing.
Associated with logging into computer systems.

C
J
N
F
C
C
M
B
1
2
3
4

Signature: Recognition based on how a person signs his name.
Associated with financial transactions.

Vascular: Recognition based on vein characteristics such as thickness and location.
Associated with security verification, such as ATMs.
Source: various companies

"It doesn't matter what security you have if the wrong person uses it," added Bill Anderson, president and CEO of Oculis Labs in Hunt Valley.

He said that until recently, cybersecurity and biometrics have been treated "very separately," despite their tight connections.

Oculis represents both sides of the security coin, with its PrivateEye product. PrivateEye offers cybersecurity technology that blurs a computer screen when the user looks away and biometric facial recognition that determines whether the user is authorized.

"The beauty of a good biometrics system is you don't have to bother the user," Anderson said.

Most laptops already have the basic components to integrate biometrics via finger keypads, cameras and voice recorders, he said. They only need a software system to utilize them.

"We layer these techniques together, since anyone can make a mistake," Anderson said. "A system needs to be adaptive to the environment."

Lockheed Martin has been involved in several biometric projects with federal clients. Its customers include the U.S. Visit Immigrant Status Indicator Technology, the FBI's Integrated Automated Fingerprint Identification System and the current Next Generation Identification, which also uses palm and face readers and is testing iris-reading technology.

The company also is researching using facial micro-expressions to detect a person's intent, which could be used in security screening. Other research areas are smell and flushed skin as stress indicators for use in crime detection.

Mears said Lockheed also is engaging with the National Institute of Standards and Technology in Gaithersburg in its effort to solicit the business world's opinions on standards for biometrics in commercial use.

And, he said, Maryland is particularly poised to take advantage of the next big thing in biometrics: DNA.

Hoping for a boost from other industries

Lockheed is getting ready to roll out a product that would allow DNA analysis via a cheek swab within an hour.

He said Maryland's booming biotech community could contribute to this next generation of biometrics.

"It could be transformational to the way we do law enforcement," Mears said.

Robert L. Wallace, founder and CEO of BithGroup Technologies in Baltimore, said he hopes biometrics becomes more linked to the cybersecurity community and its benefits, as the industry evolves.

"In our view, every institution will embrace biometric technology," he said. "I see nothing but an upside."

The BithGroup has 20 employees in its biometrics division, which provides fingerprinting analysis for background checks. The company also can perform retinal and facial scans.

Biometrics is only a 5-year-old initiative for the BithGroup, which offers technology services to solve business problems in information and energy areas.

Other executives say biometrics has a weak link with cybersecurity.

Frank Sjolie, sales engineer with Ark Systems in Columbia, argues that biometrics focuses more on identity, while cybersecurity focuses on protecting information. His company installs biometrics as part of physical access control to areas and covers retinal scanners, palm readers and fingerprint scanners.

Not so big in the U.S.

Americans have heard for years how biometrics would someday transform how they conduct their personal and professional lives. Soon, there would be no need to carry around bank debit cards and keys, they were told — or need to remember scores of computer passwords to access bank accounts or read a newspaper online.

But in the U.S., biometric applications remain limited compared with the rest of the world, for a variety of reasons, Collier said.

Hong Kong airports already have turnstiles that use fingerprint readers; the United Arab Emirates uses a 10-digit fingerprint scan to monitor foreign visitors; and India is embarking on a program to develop identification smart cards using 10-digit fingerprint and retinal information and a digital face photograph for its 1.2 billion residents.

“The U.S. leads the world in development of biometrics and is dead last in the adaptation of the technology,” said Collier, who has been in the industry for more than 36 years.

Collier also is a co-founder of the International Biometrics and Identification Association in Washington, D.C., and executive director of the Biometric Foundation, and he helped found the Center for Identification Technology Research at West Virginia University.

North America accounted for 38 percent of the global biometric market share, the largest single portion, according to a 2011 report by Evermedia Biometrics of Boston. Although the U.S. lags other regions, many ATMs in Mexico use finger scanners to verify identities. The same systems can be found in Japan, Africa and, most recently, Poland.

Globally, the public sector accounts for 59 percent of the biometrics market, according to the 2011 report.

Although the U.S. banking industry views finger-scanning technology as one option for the future, it is still working to overcome the public perception of biometrics as an invasive technology, said Doug Johnson, vice president of management policy for the American Bankers Association. The trade group represents 95 percent of the assets held by the nation’s commercial banks.

Johnson said his industry’s opinions about biometrics are changing just as some ATMs are nearing the end of their life cycle. Biometrics could be incorporated into new machines, he said.

“Clearly, we are concerned about ATM skimming. We want to do everything we can to prohibit those types of fraud. This is one solution,” Johnson said. “It’s all about layers of security.”

The Maryland Bankers Association declined to comment.

As for privacy concerns, most of the data gathered through casual biometrics are not going to reveal where a person lives, for example, Anderson said.

Collier said the U.S. continues to be held back by the notion that the technology has to be perfect before it can be adopted on a widespread basis.

“If we applied the same standards to cell phones, we still wouldn’t be using them,” he said.

Several states already have adopted identification systems using biometrics, mostly for monitoring entitlement programs such as food stamps. Los Angeles, the pilot county for using biometrics to verify entitlement beneficiaries, saved $66 million in its first three years, according to a report submitted to the U.S. Department of Agriculture.

Sjolie said the real challenge in incorporating biometrics in the mainstream lies in bringing down the cost of the technology.

Collier said he believes the U.S. need for convenience eventually will win out over other concerns, as people realize how easy biometrics can make activities.

Maryland lags For now, most biometrics companies face an unsteady market, with many Maryland companies partnering their biometrics work with more conventional consulting or security services.

"It's necessary in the evolving market to maintain viability with a mix," Kozlay said. "It has taken longer for biometrics to establish itself than many companies expected."

Maryland, with its handful of biometrics companies, also must clear some hurdles to assert its place in the biometrics market. Although the state hosts, or is near, numerous federal agencies, most biometrics companies are outside of Maryland. Even the University of Maryland, College Park, with its focus on cybersecurity research, cannot compete with the biometrics degree program offered at West Virginia University.

"It's a very active area of research. ... We'll probably pursue it in the future," said Rama Chellappa, a Minta Martin professor of engineering and interim chairman of the electrical and computer engineering department at the University of Maryland.

The university is researching face recognition biometrics, particularly in maritime environments for Coast Guard work.

Chellappa instructs a 20-student specialty course in biometrics. He also helps students build a portable facial recognition device to convey nonverbal expressions to the blind.

lrobbins@gazette.net

Post a Comment

Terms of Service

You must **LOG IN** before you can post comments.

Number of Comments: 0

Click to Show or Hide Comments
Be the first to comment.