BIOMETRIC SUMMIT
NEW YORK 2019

Hosted by
rise new york
Created by
BARCLAYS

GOLD SPONSORS

iproov zwipe

SILVER SPONSORS

AWARE PRECiSE

acuant | B Secur Connecting Your Heart | BehavioSec | noknok | ID R&D | IRIS ID | typingdna

Thursday 4 APRIL 2019

MEDIA PARTNER
BIOMETRIC UPDATE.COM

STRATEGIC PARTNER
IBIA International Biometrics+Identity Association

BIOMETRIC SUMMIT NEW YORK 2019

Biometric technology is proving to be an important tool to accurately identify people and aid the fight against fraud. We spoke to experts at Acuant, BehavioSec, Iris ID and Nok Nok Labs who represent some of the exciting technologies in this space to discover more about their innovative products and solutions and how they are set to improve everyday life both now and in the future.

Dr. Neil Costigan, CEO, BehavioSec

The last few years have been very exciting for us as we've brought Behavioral Biometrics from being a research subject to it being part of the core infrastructure for some of the most prestigious companies in the world. Looking forward, while demand is strongest from the financial sector, as ransom and malware are expanding the need for security across verticals, we're also seeing increased interest from new areas, like the healthcare industry. I think we'll continue to see exciting innovation with passive biometrics and continuous authentication over the coming years.

Machine Learning (ML) and Artificial Intelligence are very important for augmenting biometric technology solutions.These are the very techniques that made Behavioral Biometrics commercially viable, and without them we wouldn't have a product. Looking beyond the use of biometric technology solutions for authentication, I believe that a lot of the technology can probably be used for many cool health and productivity solutions. We've already seen how biometrics are used to simplify our everyday lives, removing burdensome physical tokens and other taxing 20th century solutions. As a Behavioral Biometrics company, we're also spared most of the fears associated with static biometrics, so we see biometric technology to be convenient, rather than creepy.

If you are planning to deploy biometric technology in your organization or products, then my advice is to make sure you don't get left behind; attackers prey on the weak. While most companies already know that they need to increase security, they're sometimes holding back out of a perceived safety of having little or nothing to lose in a cyberattack. Today, even the least mature enterprise holds a lot of information in CRM systems, email and internal communication tools. A leak could very well be catastrophic. Deploying a modern multilayer security system is a cheap way of reducing that risk.

Stephen Maloney, Executive VP of Business Development & Strategy, Acuant

Acuant has grown rapidly over the past few years with our cloud and mobile offerings leading the way and we've been recognized for our product innovation, including being named a Gold Winner for both the Stevie® Awards and Info Security Product Guide's Global Excellence Awards®. Importantly, our identity verification is increasingly being called upon to augment or replace traditional methods of identification such as passwords, knowledge-based authentication and data.

In our experience companies are looking for thoughtful, well designed and fully integrated solutions to solve their problems. In identity verification, proving the identity of a user, especially those not present, is becoming a business imperative. But these solutions must strike a balance between risk and friction as well as protecting personally identifiable information (PII) and regulatory compliance. We see use cases and scenarios requiring different solutions. For Acuant it is about using robust document authentication and biometrics like facial match to create trust anchors. The balance of risk and friction will then determine how it is used in onboarding good, new customers, providing people and machines with access, meeting regulatory requirements and fighting fraudulent transactions. Additionally, the use of blockchain and other cryptographic methods will allow us to carry out digital transactions while revealing only the amount of PII absolutely required for that specific transaction.

Machine Learning (ML) and Artificial Intelligence are augmenting biometric technology and aid in both big data analytics and behaviour biometrics. Our document authentication is curated machine learning with new improvements being routinely developed. We see that various use cases, guided by the level of risk and assurance required along with how much or little friction can be tolerated in the transaction, determine which technology is appropriate and how often ML or AI is utilized. We see the emergence of cloud-based AI technology will continue to make it easier and less expensive.

Looking beyond the use of biometric technology solutions for authentication, we see these technologies entering into everyday life by helping with school attendance, voice technology in automobiles and in the living room, advances in healthy living and lifestyles, near real time language translation as well as many other applications. When looking at the use of biometrics to improve everyday life, the use case helps to separate creepy from convenient. When it protects me, reduces my friction and alleviates risk, it is convenient. When it predicts or assumes things for me, follows or anticipates, it can be creepy. When it is convenient it will be used and when creepy, it will need to be regulated or dissolve.

Acuant's Next Gen Identity Platform is powered by AI with human assisted machine learning to reduce fraud while providing a seamless customer experience in the digital economy. Built to scale and meet KYC, AML & GDPR regulations, Acuant has the industry's highest speed and accuracy rates. Solutions are omnichannel allowing businesses to establish identities on premise or remotely in seconds while protecting customer data.

Contact Acuant and mention you attended the Biometric Summit for a customized identity proofing consultation.

For more information
Visit: acuantcorp.com
Email: info@acuantcorp.com

Tim Meyerhoff, Director, Iris ID

Over the past years we have seen most of our growth at Iris ID in the ID markets, specifically border patrol interdictions, legitimate border crossings, National ID and election defence applications. This year's highlight was the one thousandth system install with US Border Patrol, along with our flagship product the new E Gates being installed for Privium at Schiopl Airport in The Netherlands. There has been a lot of attention to facial recognition recently and it is an important market trend for the future. Face is part of our repertoire and although it still has issues at scale, we expect to see many more programs which will be collecting iris along with face.

Looking at what the next 'big thing' will be, in domestic US I would say it is the Air Exit pilot programs which are certainly getting a lot of attention in the media. Plus the CLEAR expansion with Hertz – biometric checkout for car rental is pretty cool. We see that there will be a lot of growth in the healthcare field along with workforce management and Access Control. Civil ID applications are on the rise globally, but slower to grow in US domestic markets. In Law enforcement & corrections we're seeing multimodal solutions now being used. For example, Face was officially implemented in the FBI database just last year and the iris pilot instituted in 2015 will be an officially supported modality at CJIS sometime in 2019.

My advice for those of you deploying biometric technology is that the overall security of the system and its ability to protect PII is paramount. Then think about the convenience of the modality, achieving a low false rejection rate, and ease of enrolment. There will be cases where a person cannot use the biometric sensor for various reasons. So accommodating ADA requirements or an alternate means of authentication should be considered. Cost is a factor of course, and the rule of 'you get what you pay for' certainly applies here.

Dr. Rolf Lindemann, Senior Director Products & Technology, Nok Nok Labs

Back in 2012 we set out a vision to transform the way authentication works, and over the subsequent years invented the concept for FIDO, recruited allies, created the FIDO Alliance and shipped the first versions of our product. Not long afterwards our vision was embraced and joined by every part of the computer industry from chips and systems to devices, authenticators and operating systems. We then created the first secure fingerprint sensor based FIDO authenticator with Validity/Synaptics, Samsung and Qualcomm and proved that FIDO could work at scale by deploying with PayPal, NTT Docomo and AliPay.

By 2018 we were the market leaders in shipping FIDO standards-based solutions with our industry-leading S3 Authentication suite. Our customers authenticate more than 150 million active users and over 4.5 billion transactions – a scale that no other standards-based authentication vendor can claim for their solutions. Our clients include four of the largest banks and four of the largest telcos in the world, and we have doubled our revenue year over year. Building on all this success, over the past year we have seen significant adoption of our technology. Some recent examples include:

• Successful launch of our S3 Authentication Suite at Japan's largest bank, MUFG Bank, Ltd
• Nok Nok S3 Suite is now used by four out of the five world largest banks
• Achieving the GSMA GLOMO Award for the "Best Authentication and Security Solution" for our S3 Authentication Suite

We're continuing to innovate around our standards-based backbone and have deployed use cases ranging from physical security and IoT applications to commerce, payments, healthcare and cloud access. And, to enable next generation authentication, we have now integrated risk signals into our product.

The future looks very exciting. We monitor developments in biometrics on three fronts: sensing technology, form factors/usability and security. We're pleased to see all three going through an explosive growth period and expect to see more biometrics, in more factors than ever before. FIDO of course allows these biometrics and tokens to be used for more than just opening your phone, it allows for secure online and privacy-respecting authentication.

Current biometric implementations already prevent scalable attacks nicely. We're particularly excited by continuing improvements in the underlying security architecture for biometrics to prevent spoofing and other targeted (non-scalable) attacks. For example, Apple and Samsung have both demonstrated careful attention to detail here using both hardware and software to innovate past previous limitations and to raise the bar for attackers. Going forward, we expect biometric vendors to put even more emphasis on presentation attack detection, given that false-accept-rates are already sufficiently low. Then, on the form factor side, we expect to see more wearables using biometrics for authentication, e.g. the rings from Motiv. It will be interesting to see if consumers will broadly accept these form factors...

Today, we are still in the early days of the post-password era. Visionary customers and early adopters are leading the way and we're now entering an era where people can trust that modern authentication is secure, scalable, easy to use and allows for privacy. We see pretty much every online interaction for consumers being transformed to use biometrics as the primary method of authentication in the next five years. Companies like Cigna, TMobile, Bank of America, PayPal and others are already doing this, and their peers in the banking, payments, commerce, cloud, media and healthcare areas will also be moving to use modern authentication based on FIDO. That brings a diversity of use cases and integrations which we are very well equipped to handle as the leading vendor in this area. For example: MasterCard Europe has been speaking about making biometrics mandatory for 3DS v2 (card not present) transactions, PSD/2 is driving a need for FIDO, NIST 800-63 which influences federal procurement is deprecating SMSOTP in favor of non-phishable authentication like FIDO. All these trends create a demand for our solutions across sectors and we have partnered with companies like Ericsson, Fujitsu, Hitachi, and OneSpan to extend our reach as this growth continues.

Other use cases and applications are set to be transformed by biometrics technology. We see demand for remote identity verification that is stronger than knowledge-based authentication (KBA). This is especially the case in countries without electronic identity cards, but even in some countries with electronic identity cards, practical alternatives to KBA are rare. As a result we see a demand for remote identity verification using biometric technology (like face recognition with appropriate presentation attack detection) typically combined with other technologies like document- scanning and document verification. If you are thinking of deploying biometric technology then I recommend you start with technologies that consumers are familiar with, and whose technology performance and security characteristics are well known. Make sure you create a threat model and understand the security and privacy model of your biometrics implementation. Consider using a mature platform that implements the FIDO specification as a shortcut to get the security, quality and privacy implementation of biometrics versus "rolling your own". An added benefit of FIDO is that it respects user preferences so both various biometric and non-biometric modalities are supported.

Finally, remember that biometrics are great to use in the case of 'local' interactions. For securing remote interactions, cryptography also needs to be part of the solution, combined with biometrics. FIDO combines both.

nok nok

Everyone, Everywhere Authenticated

Cost-Effective | Secure | Scalable | Standards-Based

JOIN US AT BIOMETRIC SUMMIT LONDON 2019

Thank you for joining us today, we hope you enjoyed this unique event and that you'll join us again later this year at Biometric Summit London 2019 on Wednesday 20 November at Rise London where we'll be extending our focus on innovation to include new sessions and engagement on biometrics for Digital Identity and Electronic Know Your Customer (eKYC).

Find out more and register at
www.goodeintelligence.com/london-2019/

BIOMETRIC SUMMIT

Hosted by

rise london