nok nok

We caught up with Phil Dunkelberger, President and CEO of Nok Nok Labs and, one of the legends from Cyber Security, to ask a few questions about the state of biometrics now and what the future likely has in store for us.

Tell us about how your business has grown and evolved over the past years.

There's been a lot happening! From 2012-2014 we set out a vision to transform the way authentication works, we invented the concept for FIDO, we recruited allies, created the FIDO Alliance and shipped the first versions of our product. Then as our vision was embraced, we created the first secure fingerprint sensor based FIDO authenticator with Validity/Synaptics, Samsung and Qualcomm. We proved that FIDO could work at scale by deploying at scale with PayPal, Docomo and AliPay. Now we're the market leaders in shipping FIDO standards based solutions, with market leading customers including four of the largest banks and four of the largest telcos in the world. And we've doubled our revenue year over year.

We've evolved the FIDO standards with Google and Microsoft, co-authoring FIDO2 to bring FIDO to browsers and operating systems and launched partnerships with Fujitsu, Hitachi, Threatmetrix and others to be announced soon who are taking our products to market.

What's the most exciting innovation you have seen in biometric technology?

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 we 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 biometrics 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 (nonscalable) attacks. Apple and Samsung have both demonstrated careful attention to detail here using both hardware and software to innovate beyond previous limitations and to raise the bar for attackers.

Where are you seeing the greatest demand for biometrics?

By far it's in reshaping customer experience and enhancing user journeys for customer satisfaction, lowered costs of interaction, greater customisation and increased profit through reduced friction.

The mobile phone has been the most popular device for consumer biometrics to date – what do you see coming next?

Mobile phones and communicators of all kinds will remain the most intense area of innovation and change. We predict changes in the form factor as battery life and radio technology get better and "unbundling" of phone features (e.g. into a data brick in your bag or a smart ear-bud you wear). In the future, biometrics will be everywhere as the "gesture" to authorise and activate these interactions.

How do you think Machine Learning (ML) and Artificial Intelligence (AI) will be used in biometrics?

Spoofing and detection of attacks is one area, more accurate template matching is another. Algorithmic techniques complemented by ML can enhance effectiveness; the challenge is doing it with minimal battery drain and to keep getting better with more use.

For those thinking about developing biometric technology, what one piece of advice would you give to them?

Keep in mind that the journey from working in the lab or limited environments to working in a commercial setting at a hundreds of millions of user scale is a long one. We've seen companies fail to integrate into required form factors, miss the quality goals, fail usability and be broken or defeated trivially in a way that would prevent any kind of mass deployment. The reason why fingerprint sensors got as good as it is, is because it took 20+ years of R&D and over a billion dollars of capital went into the sector.

And for those looking to deploy biometric technology in their organisation, what are the key things that you would advise them to consider?

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 FIDO as a shortcut to get the security, quality and privacy implementation of biometrics vs. "rolling your own".

nok
nok

Strong Customer Authentication Made Easy

Phishing Resistant | Decentralised | Privacy Ready