Entersekt

BIOMETRICS & STRONG AUTHENTICATION

Everyone with a stake in digital banking security has been tracking the rapid developments in biometrics and debating the technology's utility in the battle against cybercrime. There's little doubt that it will play an important role in securing digital services, particularly when viewed from the perspective of user convenience. But it is also fair to point out that biometrics can place enterprises and their customers at risk if deployed as the sole means of user identification and transaction authentication.

Entersekt, a leader in mobile-based authentication, offers this white paper as an account of the strengths and weaknesses of biometrics, where it works and where security professionals must augment it with other advanced counter-fraud measures.

One factor to rule them all?

Using your fingerprint or voice as a no-fuss means of digital identification makes sense. You always have these personal attributes with you and the technology conveniently eliminates a number of keystrokes, which is particularly welcome on the mobile phone. It's little wonder its popularity is spreading as fast as technical improvements and economies of scale allow.

Biometrics-based authentication promises improvement on the security offered by passwords and PINs, but banks' primary interest in the technology relates to usability: it reduces the amount of information users have to input manually. Instead of having to type out login credentials or awkwardly switch between apps to enter a one-time password, users can access their accounts and approve transactions with a quick scan of a fingerprint or voice.

A recent report by London-based analyst firm, Goode Intelligence, estimates that by 2017, more than a billion users will have provided biometric information to access banking services. The report also predicts that, within the next four years, biometric data will become the personal identifier of choice for consumers accessing their bank accounts.[1] Research by Experian has revealed that 61 percent of UK adults already believe biometric identification is either just as secure or more so than passwords, and 40 percent would be happy to use fingerprint scanning to access their online accounts.[2]

Associated webinar with Alan Goode

This white paper draws content from an Entersekt webinar featuring independent analyst and biometrics expert, Alan Goode. Watch the complimentary recording to learn about top trends in biometrics authentication and relevant industry standards. Also examined are the options banks have for boosting the security of mobile-based biometrics without adversely affecting the user experience.

***One factor to rule them all? Biometrics and strong authentication*.**

Goode Intelligence estimates that there will be 622 million mobile banking apps that offer biometric authentication by 2020, with $5.6 trillion in payments being secured by biometrics. According to WinterGreen Research, the global biometrics market will be worth $44.2 billion by 2021.[3]

Voice recognition technology has been in use by Tatra Bank in Slovakia since 2013. RBS and NatWest in the UK have been offering fingerprint authentication for the past year. HSBC, also in the UK, will start to allow voice pattern recognition and fingerprint reading as identity verification measures this year. Al Baraka Bank in Pakistan recently completed their testing of a new biometric verification system for transaction approvals and other actions. MasterCard even plans to roll out a

[1] "Goode Intelligence names five key drivers of biometrics adoption for financial services" (February 4, 2016); Justin Lee; *Biometric Update* [http://www.biometricupdate.com/201602/goode-intelligence-names-five-key-drivers-of-biometrics-adoption-for-financial-services]

[2] "UK now ready for biometric banking" (January 13, 2016); Experian press release [http://www.cutoday.info/Fresh-Today/In-Survey-Most-Say-They-Are-Ready-To-Embrace-Biometric-Security]

[3] *Biometrics: Market Shares, Strategy, and Forecasts, Worldwide, 2015 to 2021* (October 3, 2015); Ellen T. Curtiss, Susan Eustis; WinterGreen Research

facial biometrics app for the authentication of online purchases. After testing in the UK and the Netherlands, 92% of users preferred the selfie function to a password. By the middle of 2016, the functionality should be available in 15 countries. MasterCard is also testing voice and iris scanning as means to authenticate credit card transactions.[4]

Same old challenge: Protecting the data

Biometrics-based authentication scores highly on ease of use and is unquestionably more secure than passwords are, but many privacy and security concerns remain. One big worry relates to where digitized biometric records are stored. Just like anything digital, this information exists as bits and bytes, which can be copied and shared with ease. Passwords and other login credentials have leaked in the billions, but will biometric data prove any safer in the long run? How do organizations prevent exposing their consumers' biometric data to the dark web and the patrons of darknet markets in stolen identity?

The risks are high. Once fraudsters have their hands on a user's digitized fingerprint, they might access other of their biometrically secured accounts or commit a range of other crimes. Many biometric traits are also irrevocable, including all attributes that are commercially viable at present. A fingerprint can never be substituted like a password or digital certificate can.

Biometrics-based authentication systems must protect biometric data where it is stored, while it is accessed, and if and when it is transmitted. Broadly speaking, there are two competing models for doing so in the mobile-oriented mass market: server-based biometric authentication and device-based biometric authentication. Below, we discuss the advantages and disadvantages of both.

Server-based biometric authentication

In the first of these models, the service provider itself captures biometrics data, and the information is stored centrally under its watchful eye. The party bearing the greatest liability thus enjoys full control of the process, architecting user authentication to match its risk appetite closely. Systems like this also allow service providers to reuse individual biometric records across all their digital channels, authenticating users of mobile, Internet, in-branch self-service, call center, corporate network, or others.

On the downside, large single-reference repositories make highly attractive targets for hackers. The potential gains in accessing a very large database are greater than for a series of smaller ones. One system presents a single challenge, one attack surface against many.

[4] "MasterCard's 'Selfie' App Aims to Replace Passwords" (February 25, 2016); Tracy Kitten; *BankInfoSecurity* [http://www.bankinfosecurity.com/mastercards-selfie-app-aims-to-replace-passwords-a-8898]

In 2006, detailed information on more than 9 million Israelis, alive and dead, was stolen and posted to the Internet.[5] Israel is arguably the most security-conscious country in the world and is home to scores of innovative digital security startups, yet the Israeli Biometric Database Management Authority has admitted that it cannot guarantee a national biometrics database, still in trial, will not be breached in future. The committee overseeing the project now recommends that only low-resolution headshots and not fingerprints be collected, fearing future security lapses.[6] In 2014, fingerprint records of more than 5.6 million past and present US federal employees were stolen from the Office of Personnel Management, together with social security numbers, contact details, and security-clearance-related background information.[7]

In Mauritius, a program to digitize the fingerprints of all citizens for use on a national identity smart card met with such stiff resistance that the central database housing this information was destroyed.[8] There were fears over how the government might abuse the information it collected, but a series of embarrassing system malfunctions also had Mauritians wondering how long it would be before their data was published online by hackers.

Device-based biometric authentication

The approach mobile industry leaders like Samsung and Apple are taking is fundamentally different to that described above. Their model, endorsed by the FIDO Alliance, requires users to self-enroll biometric information using their mobile device. The data, crucially, never leaves the phone.[9] This model addresses many of the privacy concerns and security risks that arise from the central storage of bulk biometric data by enterprises and governments.

One drawback to not sharing biometric data beyond the mobile device is that the identity of the user cannot be guaranteed. Unable fully to access and match the data to its own records, the service provider cannot definitively know that the user is the legitimate party in any communication. All it can determine is that an individual who registered their fingerprint on a particular device has just scanned it successfully.

Or have they? Researchers have demonstrated the ability to spoof fingerprints using everyday materials like inkjet printers and conductive ink, children's modelling clay, wood glue and, back in

---

[5] "Population Database Hacked in 2006 Reached the Internet" (October 25, 2011); Jonathan Lis; *Haaretz* [http://www.haaretz.com/population-database-hacked-in-2006-reached-the-internet-1.391812]

[6] "Israeli biometric database authority acknowledges potential security flaws" (March 23, 2006); Stephen Mayhew; *Biometric Update* [http://www.biometricupdate.com/201603/israeli-biometric-database-authority-acknowledges-potential-security-flaws]

[7] "OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers" (September 23, 2015); Andy Greenberg; *Wired* [http://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/]

[8] "Mauritius NIC Biometric Data To Be Destroyed" (January 30, 2015); *Island Crisis News* [http://news.islandcrisis.net/2015/01/mauritius-nic-biometric-data-to-be-destroyed/]

[9] The FIDO Alliance (Fast IDentity Online) is a consortium responsible for the first standards-based open protocol for online authentication. Entersekt was an early member. [https://fidoalliance.org/specifications/overview/]

2002, gelatine.[10] [11] [12] In reporting the latter case, renowned cryptographer Bruce Schneier wrote bluntly, "The results are enough to scrap the systems completely, and to send the various fingerprint biometric companies packing."[13]

We have come some way since then, but the vulnerabilities are still real. The scanning and storage of biometric data, in this model, leave banks dependent on mobile device manufacturers, on their assessment of the precision of their sensors and the security they deem to be adequate. Where a server-based approach allows banks to conduct the enrollment of their customers and bind their attributes to their customers' accounts, a device-based model cedes control to third parties. Risk officers across the industry view this as a dangerous proposition.

Biometrics is most commonly used to authenticate banking customers at login. Security concerns are retarding progress on extending the technology's applicability to transaction verification and digital document signing. Allowing users to unlock their mobile banking app with a fingerprint is one thing but, for sensitive transactions like adding a beneficiary or making money transfers, banks usually revert to older, less convenient forms of authentication.

Combining biometrics with other factors

> *Mass market biometrics are currently only about convenience, not security. Not having to remember PINs is nice, but relying solely on biometrics is hazardous. Security is added, or rather implemented, by combining other factors (something you have, something you know), but here is the catch – the more you secure, the less convenient is the solution.*
>
> ***— Arvin Ramkhelawon, senior consultant, Consult Hyperion[14]***

[10] "Hacking Mobile Phones Using 2D Printed Fingerprints" (February 19, 2016); Kai Cao, Anil K. Jain; Michigan State University [http://www.cse.msu.edu/rgroups/biometrics/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf]

[11] "Are mobile payments gambling with consumer identities?" (March 1, 2016); André Malinowski; *ITProPortal* [http://www.itproportal.com/2016/03/01/are-mobile-payments-gambling-with-consumer-identities/]

[12] "Computer Chaos Club breaks Apple Touch ID" (September 21, 2013); Computer Chaos Club blog [http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid]

[13] "Fun with fingerprint readers" (May 15, 2002); Bruce Schneier; *Crypto-Gram* newsletter [https://www.schneier.com/crypto-gram/archives/2002/0515.html]

[14] "Mass market biometrics – convenience and trust" (September 14, 2015); Arvin Ramkhelawon; Consult Hyperion blog [http://www.chyp.com/mass-market-biometrics-convenience-and-trust/]

Although biometrics-based authentication has its shortcomings, none of these invalidates it as a security tool. No single security measure will hold for long against persistent attacks from cybercriminals and other mischief-makers. Other methods of establishing identity must supplement a biometrics-based solution – and must do so without impacting negatively on the user experience.

A two-pronged security approach is typically used to protect digital banking users' private data against cyberattacks. To log in to their online or mobile banking, they must first identify themselves. Next, they must prove that identity through authentication. Effective security strategies are made up of two or more of the following factors of authentication:

- Something the user knows: a password, PIN, answer to a challenge question (mother's maiden name, first pet's name, etc.), even a secret handshake
- Something the user has: a front-door key, debit or credit card, mobile phone, or USB token
- Something the user is: a scan of their fingerprint, palm, retina, voice. This can even be extended to so-called dynamic biometrics, such as signature recognition or gait analysis, and social biometrics, which authenticates a user based on their historical behavior (the way they hold their device, say, or the websites they visit.

So, while biometric data helps identify the user, a second factor of authentication must be in place to verify that identity and the user's intention to carry out a specific transaction. Kevin Curran, a senior member and security expert at IEEE, explains it this way:

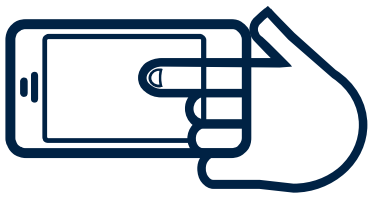
> "One technique which should be combined with any biometric authentication is a multi-factor one. This reduces risk by involving separate types of factors that would require an attacker to use different methods of attack, thus making a breach more difficult. Multi-factor authentication combines at least two of the following methods to strongly authenticate a user: something you know, which is typically a password or PIN; something you have, like a trusted device identifier that is not easily duplicated; and something you are – in other words, your unique biometrics.
>
> "Two items must be combined from different categories in order to qualify as multi-factor authentication, so a PIN plus a password is not actually multi-factor, since both of these are something you know. Full three-factor authentication, when combined with a device ID, allows users to easily combine 'what we have' and 'what we know' with the important 'who we are'. This is hugely important for future security systems."[15]

[15] "The role of biometric authentication techniques in security" (April 7, 2016); Kevin Curran; *ITProPortal* [http://www.itproportal.com/2016/04/07/the-role-of-biometric-authentication-techniques-in-security]

Entersekt's unique approach

"If the biometric is paired with device identification, this is as secure as you can get."

— Shirley Inscoe, senior analyst, Aite Group[16]



Entersekt's solutions support biometrics on iPhone and Android Marshmallow mobile devices but, in agreement with peers in the industry, we believe that it should be only implemented as part of a layered security system. Fingerprints and other biometrics can be a significant additional tool in our efforts to deter account takeover activity, but only when deployed as part of a multi-factor authentication regime. With this goal in mind, Entersekt supports biometrics to replace the user ID/password and act as an additional data point in mobile-based out-of-band authentication.

To guarantee that the user is legitimate and that their communications are those that they intended, the mobile device itself must be uniquely identified using a unique digital certificate, just as the enterprise is. The device is, in this way, transformed into a trusted second factor of authentication (something the user has) supplementing the first factor, the device-bound biometrics data (something the user is). User communications can then be signed by the digital certificate unique to the phone, and all transmissions between the device and the enterprise encrypted from end to end.

All of this is possible with Transakt, a patented, push-based authentication and app security product from Entersekt. By means of an SDK (software development kit), Transakt integrates seamlessly with any bank's existing mobile banking app, enabling the bank to provide a feature-rich app, protected with industry-leading mobile app security. As an early member of the FIDO Alliance, Entersekt supports its vision of mobile biometrics-based authentication resting on user self-enrollment and device-bound data storage. Transakt is FIDO Certified™ as a U2F (universal second

IEEE's standard 2410-2015 or BOPS (Biometrics Open Protocol Standard) is a global standard for digital identity and authentication that is, in essence, a competitor protocol to those developed by the FIDO Alliance.

[16] "MasterCard's 'Selfie' App Aims to Replace Passwords" (February 25, 2016); Tracy Kitten; *BankInfoSecurity* [http://www.bankinfosecurity.com/mastercards-selfie-app-aims-to-replace-passwords-a-8898]

factor) authenticator. It allows enterprises to apply a device-based biometrics authentication model without ceding control of the security of the solution to device manufacturers, app developers, mobile networks, or other third parties.

With Transakt, mobile users can opt to use biometrics on their mobile devices but benefit from added protection that in no way impedes them in completing transactions quickly. Once logged in using a fingerprint or other biometric trait, users authenticate their transactions by responding to a simple prompt pushed to the phone in real time. This message, which overlays their mobile banking interface, contains concise details of the transaction they initiated, and all the user has to do is tap “Accept” to complete it. No passwords are required. “Reject” cancels the transaction immediately, should the user suspect criminal activity.

From the banks’ perspective, this approach not only secures their mobile banking app beyond anything biometrics can provide alone; it meets their requirement for a low-friction user authentication process.

Further reading on entersekt.com

Solution sheet: *Mobile banking authentication*
[https://www.entersekt.com/Mobile-Banking-Authentication-Solution]

White paper: *Muscling up on strong authentication: Best practices*
[https://www.entersekt.com/Muscling-up-on-strong-authentication]

White paper: *Securing the mobile banking channel*
[https://www.entersekt.com/Securing-the-mobile-banking-channel-White-Paper]

Entersekt, Tower Place 100, Suite 620, 3340 Peachtree Road NE, Atlanta, GA 30326, United States

Phone: +1 404 698 1001 E-mail: info@entersekt.com

Web: www.entersekt.com

Document ID: ENTERSEKT-40-1367