FORESIGHT

8 Mill and Main Place, Suite 150 | Maynard, MA 01754
www.mercatoradvisorygroup.com |phone 1-781-419-1700 |email: info@mercatoradvisorygroup.com

April 2017

BEHAVIORAL BIOMETRICS WILL RESTRUCTURE THE AUTHENTICATION LANDSCAPE IN THE NEXT 5–8 YEARS

Behavioral biometrics can persistently authenticate a user utilizing existing mobile sensors. This will finally eliminate passwords.

Persistent multifactor identity based primarily on behavioral biometrics can be established using sensors that already exist in the vast majority of smartphones in market. This will irrevocably alter the authentication landscape and will enable entirely new players to become authentication market leaders.

by Tim Sloane,
Vice President, Innovations, and
Director, Emerging Technologies Advisory Service

Introduction

Solution providers of technology that enable authentication of users, including ID verification solutions, password management and recovery solutions, access control solutions, smartcards, and stand-alone biometric scanners are facing a major technological change that will decimate much of the existing authentication market. As a result, entities responsible for border security, civil ID, electronic security, computer access controls, physical access controls, financial services, healthcare, law enforcement, military, payments, and workforce management will all be forced to grapple with the fact that existing authentication solutions are quickly becoming obsolete and will be displaced by new technology within just 5 to 8 years. This is particularly true for any biometric solution that utilizes centralized storage of biometric credentials, since maintaining this honeypot is a risk that every organization should avoid at all costs and that consumers should flatly reject.

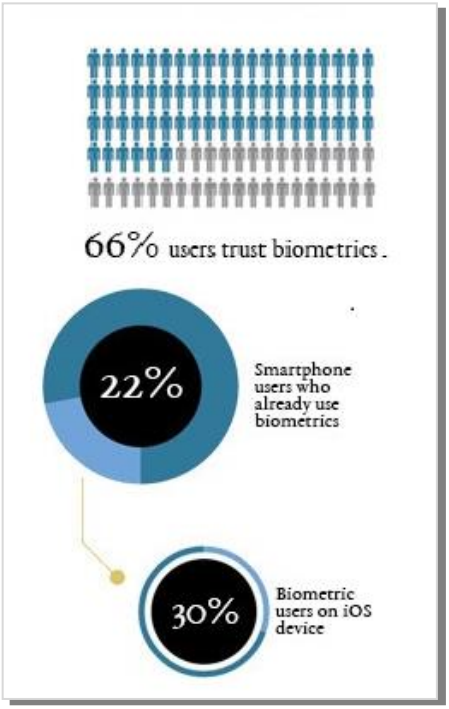
How any given solution is positioned to survive this tsunami over the next 5–10 year time frame depends primarily on how the solution manages trust in the mobile environment. If the current solution isn't positioned to take advantage of the highly trusted hardware-based security vaults being deployed in the mobile handset, then that solution will be antiquated within 5 years if not sooner. If the current solution utilizes trusted hardware combined with physical biometric readers, then the impact is more likely to be felt in 6–7 years, which is still well within the breakeven time frame for return on investment, or ROI, for most large hardware-based biometric solutions deployed today.

The solution driving this disruption is persistent identity within the smartphone, which is combined with a token embedded in the mobile device's secure hardware and secure operating system. While it remains unclear exactly which biometric signals will be implemented, future authentication will almost certainly incorporate a combination of behavioral inputs, sounds (which are likely to include voice recognition and ambient sounds), geolocation data, and perhaps facial recognition. These inputs will be used to formulate an identity trust value utilizing machine learning tools. This will happen quickly because this implementation utilizes the existing capabilities of smartphones.

How Quickly?

Mercator Advisory Group has recently released two reports on the future of biometric authentication. The first, *Biometrics: A New Wrinkle Changes the Authentication Landscape*, explains how the huge market shift to biometrics will restructure the authentication market. The second, *Biometrics: A Market Forecast for Consumer Adoption,* provides a forecast for the growth of the mobile-based biometric solutions that will displace traditional solutions utilizing behavioral biometrics, traditional biometrics, consumer data derived from the cloud, and machine learning tools that will analyze all of this data to establish a persistent identity trust metric.

This isn't science fiction. While many details remain foggy (such as which providers will enable federation and how the identity metric will be developed, measured, and delivered), the outcome is obvious because of basic economics combined with consumer behavior.

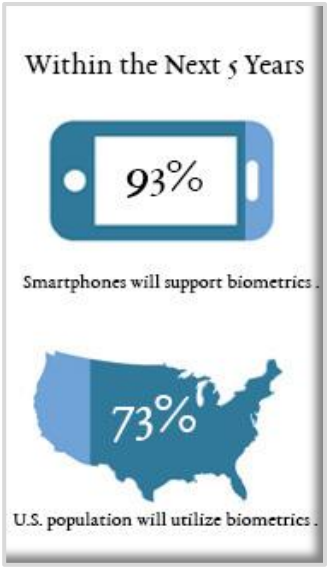


Mercator Advisory Group's survey research indicates that 22% of U.S. consumers over age 18 with a smartphone already use biometrics on the device they own. The use of biometrics is limited, of course, to smartphones in market that have the appropriate hardware. If we only consider owners of Apple devices that support Touch ID, we find that 30% of owners were using it as of June 2016.

The primary reason that biometrics has not been more widely adopted is that it offers the consumer very little value in the way of convenience. Today the biometric unlocks the phone, a wallet, and perhaps a few additional applications. But adoption will climb rapidly in the future when the biometric unlocks not just the device but all of the mobile applications on that device, including bank apps, and all other password-centric solutions including websites, and does so in most cases without a challenge to the device holder. We are certain of this increased adoption rate based on the adoption pattern observed with mobile banking, which delivered far less consumer convenience. According to Mercator's 2016 survey, 66% of smartphone users in the U.S. indicated that they trust biometrics. Another 18% indicated they didn't care about security at all, but they do care about convenience!

Key Assumptions of the Mercator Biometric Forecast

In order to track consumer acceptance of this new authentication capability, Mercator identified several high impact issues that will need to be tracked to assure the forecast stays on track.



Trusted Security in Mobile Devices

Apple, Google, and Samsung are all moving rapidly to shore up security of their mobile devices and mobile operating systems. In the reports cited earlier, Mercator Advisory Group details the assumptions associated with the deployment of this secure environment and tracks the market penetration in combination with device support for biometrics. These are linked because Google requires device manufacturers to implement a hardware trusted execution environment if they include a fingerprint sensor or other biometric sensor. Our forecast indicates that over 90% of phones in market will include some biometric by 2023.

Federation and Persistent Identity

Convenience is a critical aspect for driving consumer adoption of biometrics, and the greatest possible convenience is derived when the same biometric transparently satisfies every authenticator with which the consumer interacts. Two issues must be addressed to make this happen. First, authenticators will need to adopt a common form of federation so the chosen biometric can be used across the widest possible range of authenticators. Many implementations of this approach already exist, but none has attracted the majority of authenticators that interact with consumers. The second issue is the reliability and convenience of the algorithm used to validate identity. The algorithm used with biometric hardware today requires a challenge to the device holder, who must then physically present the biometric.

By utilizing behavioral biometrics, the challenge/response approach can be replaced with a persistent identity. The mobile device monitors the user's voice, face, gait, typing style, and other information sources to constantly create a trust metric that is available as required for authenticators willing to utilize that metric for their own access control infrastructure.

In this scenario of federation, the consumer's device can be queried and if the trust factor is sufficiently high, or the accessed service sufficiently low risk, then access can be granted without the need to challenge the user. A user would be able to access her bank balance or withdraw $100 without being challenged but would be challenged if she tried to transfer $2,000 out of the account. The Mercator forecast predicts that 90% of the mobile phones in market in 2023 will have support for persistent identity.

Federated Identity Explained

A web-based account is protected by utilizing user IDs and passwords. These identity systems are generally not interoperable. The lack of interoperability prevents a user from accessing multiple systems using a single user ID and password.

Federated identity solves this interoperability problem and enables organizations to share trusted identities across the boundaries that separate them. The details and complexity of the identity systems of each organization are hidden from the others utilizing standards. Current operational solutions are being standardized, which includes the OASIS SAML TC, the Liberty Alliance, and WS-Federation.

Consumer Adoption

The infographics shown in this ForeSight report are derived from the Mercator Advisory Group's Consumer Monitor Survey Series (CMSS), which provides a representative sample of the U.S. market. This survey is conducted twice every year, and so we will be monitoring consumer adoption of biometrics very closely. As already described, adoption will be driven by availability of a capable device, increased adoption of biometrics by authenticators, and the availability of persistent identity, all of which this ForeSight predicts will be well advanced by 2023. So the next challenge is predicting how quickly consumers will adopt this new authentication method once it becomes available.

The model used to predict consumer adoption of persistent identity is directly based on the adoption rate measured for mobile banking. Mercator's CMSS research tracked consumer attitudes and concerns regarding mobile banking as well as the actual usage of mobile banking from 2011 through 2014. Over that 4-year period, consumer trust in mobile banking increased by 21% and consumer usage of mobile banking increased by 33%. This rise in adoption was driven, in part, by convenience and the direct marketing efforts of the banks. Mercator fully expects that consumers will adopt persistent identity much faster than they did mobile banking. We expect this based on the convenience provided to consumers by the ability of persistent identity to unlock their mobile devices and mobile applications as well as the vast majority of their password-protected websites. Despite this expectation of faster adoption, Mercator used the exact same adoption rate that we measured for mobile banking to generate this forecast for adoption of persistent identity. Based on that model we expect that in 2023, 72% of smartphone users will utilize persistent identity.

The Mercator research report *Biometrics: A New Wrinkle Changes the Authentication Landscape* details the technology and solutions that will establish this new authentication landscape. The speed of deployment and adoption is driven by availability. And because authentication through persistent identity is a cloud solution that utilizes behavioral biometrics via sensors already in the smartphones deployed around the world, this new authentication method will be adopted very quickly. Any delay in broad consumer adoption of biometrics isn't likely to be technological. Rather, any delay will likely be caused by the inability to utilize biometrics to unlock the broadest possible range of apps and websites. That this obstacle continues even today is totally illogical given the benefits and the ease of implementation.

Related Concerns

If you find this piece of interest and would like to explore this issue further, possible proprietary project work could be done to examine questions like these:

What will the authentication value chain look like in the future, and with what impact on your firm?

How will cloud authentication affect existing solutions, and how should authentication solutions be deployed to leverage this shift?

How can behavioral biometrics be implemented to protect online assets while enabling a smooth transition?

What is the likely impact of "zero-knowledge proof" algorithms on existing identity solutions?

What will be the impact on current and future investments in authentication technology?

How can your organization take advantage of this market shift?

How will the transition affect operational systems and customer interactions across all channels? Which channels first?

How might an organization leverage the concept of self-sovereign identity to establish a consumer-friendly, differentiated market position?

Let Mercator Advisory Group help your company become better positioned in the market.

Contact us:
1-781-419-1700 or email:
info@mercatoradvisorygroup.com

Biometric Authentication: Easy to Implement with Significant Benefits

Developers of apps and websites today have yet to embrace biometrics for their own solutions despite the fact that very little effort is required by developers to unlock a mobile app using a fingerprint. The Android solution website offers 14 lines of code that developers utilize to enable fingerprint authentication. The entire developer library for Apple's Touch ID code is just 34 KB.[i] Complexity is clearly not what is preventing adoption by developers.

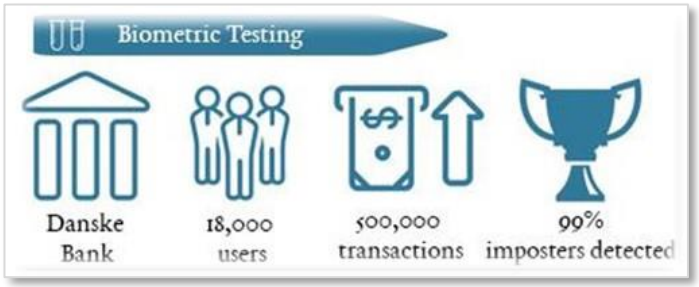
Perhaps business managers are simply unaware of the benefits available when fingerprints are used to provide a better customer experience. Here are a few examples of such benefits that Mercator pulled from the SmartLock page on the Android developer website[ii]:

- HotelTonight: Conversion rates up 23%.
- Netflix: A 20% reduction in contact volume from members unable to sign in using Android devices.
- AliExpress: An 85% drop in sign-in failure rate.
- The Guardian: A 44% increase in cross-site access.
- Ticketmaster: A reduction in manual sign-in failures from 40% to 50%.

All of these are benefits for both the consumer and the authenticator. The effort is low and the benefits very high, so the delay in adoption is hard to comprehend. Of course, it would be far better if the same benefits could be applied to the password-protected websites that we visit, as that would be far more convenient and hence drive much greater consumer adoption.

The Intersection of Technology, Consumer Trust, and Regulation

Recognize that a range of confounding factors will make the exact path for the deployment of persistent identity difficult to plot. While it appears that Google and Apple are best positioned to deliver persistent identity and the commensurate federation service, it isn't clear that this will happen or is a priority for them. The Google Abacus project is said to be in pilot with banks and universities, but no details have been released since the demonstration by Regina Dugan, Head of Google ATAP and former director of DARPA, at Google I/O in 2015.



As a result of its control over the hardware and OS environment, Apple has achieved a lead in both hardware and operating system security. In addition, Apple's focus on keeping all personal data within the device encrypted and eliminating backdoors as much as practical has won praise from consumer advocates, but this approach may make it more difficult for Apple to apply machine learning to all the user data. Keeping user data in the handset also makes it difficult to gather training data utilized to improve the machine learning algorithm. Given the current capabilities of machine learning, many of these functions are likely better executed in the cloud. But of course a cloud implementation raises consumer privacy concerns.

Multiple solutions exist, as there are several well-known software methods available to federate multiple sites under a single authentication solution, but so far no company has had enough clout to attract all of the independently operated websites. Amazon, Facebook, LinkedIn, and others have tried to promote their authentication methods as a standard across multiple websites, so any of these might decide to expand its current solution to incorporate biometrics. Even if they do, it is also possible that PayPal, Visa, or some other large and trusted player might step in. If not, then it is likely that the role will fall to Google and Apple as the likely providers. It is telling, however, that consumers who own Apple and Samsung fingerprint-enabled mobile devices must still remember their passwords when they access websites from those very same companies. While the current operating systems make it difficult to properly provision the device so that a specific user is tightly coupled to a specific fingerprint, this situation makes no sense since Apple, Google, and Samsung control the entire solution.

So while Google may find that it can advance persistent identity by evaluating user metrics in the cloud, this might in turn provoke resistance from consumers, who may perceive a cloud solution as putting user privacy at risk. It is clear that these are not idle concerns. Several states, in response to consumer concerns, have already passed legislation intended to protect consumer biometric data, and such legislation is likely to further extend product release dates.

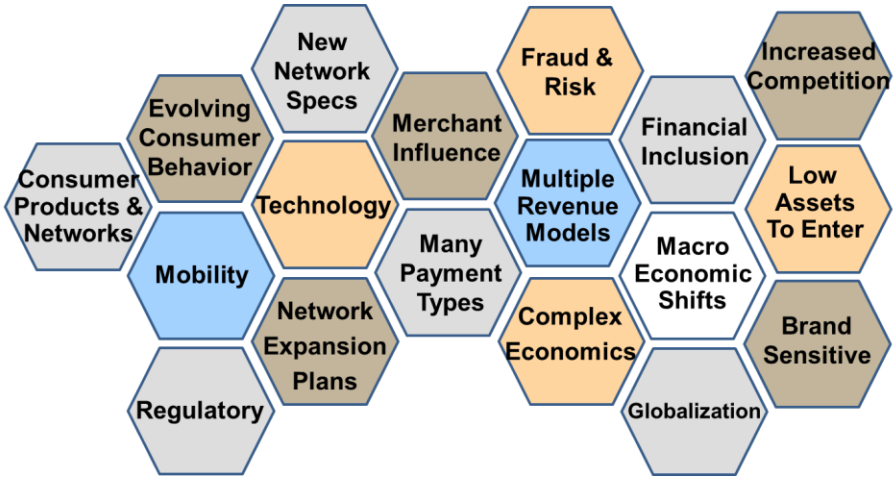
Over time, new technologies may evolve that eliminate the need to release biometric data outside of the smartphone. As an example, Google recently announced a chip[iii] that implements its machine learning algorithm (TensorFlow) with greatly increased speed while reducing power consumption. Nvidia has done the same with its new Pascal P40 chip.[iv] While Apple is unlikely to utilize a chip from its primary competitor, this development suggests that Apple could implement persistent identity within the iPhone utilizing the Nvidia chip in a future version.

As already noted, it will be important to keep all biometric data within the smartphone, as has been promoted and defined by the FIDO Alliance. Yet there are other technological approaches. One is the "zero-knowledge proof," which is available as open source software from Microsoft (the U-Prove implementation). A zero-knowledge proof enables a consumer to prove to an authenticator that a given statement is true without conveying any information. For example, the authenticator could ask if the user's smartphone is located near the laptop being used to access a website. The response confirms or denies the statement without revealing where the smartphone is actually located. While statements to be validated must be established in advance and standardized, such an approach offers clear advantages to solutions requiring that the user's details be provided to authenticators.

As with federation, however, the problem here is a lack of broad adoption. The existence of too many different solutions can be as difficult to overcome as no technology at all. This problem will be resolved if ever a major industry player establishes a value proposition that is impossible to resist. Again, if the same solution existed on every handset, the adoption problem could be quickly resolved, though not necessarily the consumer and regulatory perception of that specific approach.

These technical, consumer, and regulatory concerns are far from the only issues likely to affect the trajectory of persistent identity as it comes to market. Figure 1 identifies a range of issues that have nothing at all to do with technology and yet every one of these may alter the way persistent identity enters the U.S. market.

Figure 1: The Many Influences That Will Have an Impact on the Trajectory of Persistent Identity



Source: Mercator Advisory Group

All of the issues identified in Figure 1 have an impact on payments in the United States, and the majority will also have an impact on the way that persistent identity will ultimately enter the market. This ForeSight report has already stated Mercator Advisory Group's intent to track the key issues impacting the Mercator forecast for persistent identity. We will also be keeping tabs on all of the issues reflected in Figure 1 and reporting back to our members any obstacles discovered. Mercator Advisory Group will also be adding a range of specific questions to our CustomerMonitor Survey Series to be able to provide updates to our members whenever we detect a major shift in patterns of consumer adoption of biometric authentication.

Conclusions: What Might Be Next

In the few days that it took to write this synopsis of Mercator's research on authentication methods, several announcements were made that advance the introduction of behavioral biometrics. Experian announced[v] that it would utilize the behavioral biometrics from BioCatch to strengthen its e-commerce authentication portfolio, Mastercard acquired[vi] NuData, suggesting that Mastercard could enable behavioral biometrics as a component of 3d Secure V2. And Vasco adopted[vii] Behaviosec behavioral biometric technology, while Morpho was acquired by Advent International, which also owns Oberthur.

The introduction of behavioral biometrics, persistent identity, and a new and compelling federation business will disrupt the entire authentication value chain—from manufacturers of sensor hardware to the authentication used to control access to computer systems and websites to physical access controls. Literally no aspect of authentication will remain untouched. Helping our members to track how this technology enters the market, when it will arrive, and how to respond is a key component of Mercator's Emerging Technologies Advisory Service.

Endnotes

[i] https://developer.apple.com/library/content/samplecode/KeychainTouchID/Introduction/Intro.html, accessed 3/3/2017

[ii] https://developers.google.com/identity/smartlock-passwords/case-studies, accessed 3/3/2017

[iii] https://www.forbes.com/sites/kevinmurnane/2017/04/10/the-great-strengths-and-important-limitations-of-googles-machine-learning-chip/#6c6e6618259f, accessed 4/17/2017

[iv] https://www.nextplatform.com/2017/04/12/googles-tpu-investment-make-sense-going-forward/, accessed 4/17/2017

[v] http://fortune.com/2017/04/07/experian-biometrics-startup-fraud-online/, accessed 4/17/2017

[vi] https://www.streetinsider.com/Corporate+News/MasterCard+(MA)+to+Acquire+NuData+Security/12718311.html, accessed 4/17/2017

[vii] https://www.vasco.com/about-vasco/press/2017/behavioral-authentication.html, accessed 4/17/2017

Copyright Notice

For more information about this report, please contact:

Tim Sloane, Vice President, Payments Innovation, and Director, Emerging Technologies Advisory Service
tsloane@mercatoradvisorygroup.com
1-781-419-1712

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver a unique blend of services designed to help clients uncover the most lucrative opportunities to maximize revenue growth and contain costs.

Advisory Services. Unparalleled independent and objective analysis in research documents and advice provided by our Credit, Debit, Prepaid, Customer Interaction, Commercial and Enterprise Payments, Emerging Technologies, and Global Payments practices.

Primary Data. *CustomerMonitor Survey Series* presents eight annual Insight reports based on primary data from Mercator Advisory Group's bi-annual surveys of 3,000 U.S. adult consumers to determine their behavior, use, preferences, and adoption of current and emerging payment methods and banking channels to help our clients identify and evaluate business opportunities and make critical business decisions. *Small Business Survey Series* presents three annual reports from Mercator's annual survey of small businesses

Consulting Services. Services enabling clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans. Offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training.

PaymentsJournal.com. The industry's only free online payments and banking news information portal delivering focused content, expert insights, and timely news.

For additional copies of this report or any questions, contact Mercator Advisory Group at 1-781-419-1700.