Factors of Authentication

There are three recognized factors of security for authentication: "something you know," "something you have," and "something you are." Most modern security systems use only one of these factors for authentication, leaving them open to attack.

However, when two or more of these methods are combined into one system, security is greatly increased. This is called multi-factor authentication. The multi-factor authentication creates a layered defense, making it more difficult for an unauthorized person to access a target.[1] If one method of authentication is compromised or broken, the attacker still has at least one more barrier to breach before successfully completing their attack.[2]

This whitepaper will explore the strengths and weakness of the authentication factors and demonstrate how Asignio's 3-factor system solves the problems of digital authentication.

[1,2] SearchSecurity. http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA.

Factor 1: Something You Know

"Something you know," or knowledge-based authentication, is the most common way of verifying identity. Knowledge-based methods include asking for passwords, PINs, or personal information—all things that only the user should know.

There are several problems with knowledge-based authentication when used on its own. The most common problem is human nature: users often have the same password for multiple accounts. The average American has over 100 accounts with login credentials, requiring the user to remember a separate password for each.[3] Remembering 100 distinct passwords is both frustrating and futile, forcing users to recycle their passwords. A Telesign survey found that 73 percent of respondents used the same password for multiple sites.[4]

In order to solve the security challenges presented by password recycling, institutions force users to constantly change and update their passwords in an attempt to strengthen security. Institutions will often require passwords with a minimum of eight characters, at least one capitalized letter, and one special character. However, most users end up forgetting these new, complicated passwords, which makes for weak security and poor customer experience.

Additionally, knowledge-based authentication is open to several methods of attack. Hackers use social engineering—phishing, pretexting, malware, or other methods—to trick users into revealing personal information and gain access to their account. Hackers also use brute force methods or direct attempts to guess a password in order to gain access. These methods are particularly dangerous because a successful attack will often compromise several accounts if the same password has been reused.

[3] TechRepublic.com. http://www.techrepublic.com/article/lastpass-the-smart-persons-guide/
[4] Telesign. https://www.telesign.com/resources/research-and-reports/telesign-consumer-account-security-report/

Factor 2: Something You Have

"Something you have," or token-based authentication, is most often used for internal corporate authentication and access control. Token-based authentication methods include ID key-cards and RFA tokens. Rather than rely on passwords and personal information that can be hacked or stolen, token-based authentication bolsters security by tying identity to a physical object. If a thief wants to access the user's accounts, they must somehow gain access to the token itself.

While token-based authentication solves some of the issues faced by knowledge-based authentication, problems exist here, too. Token-based authentication works well for access control, but struggles to meet the modern challenges of digital authentication. Many token-based authentication methods do not work with mobile devices and cannot be used cross-device.

Beyond the inconvenience of forcing users to constantly carry around their tokens, institutions must find a way to handle high support costs. When a token is misplaced, the institution must have an efficient support system in place to help the user. Each time a token is lost, the institution must move quickly to invalidate the old token and distribute a new one in order for the user to continue their work. If this is not done, the user's account is at high risk for fraudulent activity.

Factor 3: Something You Are

"Something you are," or biometric authentication, is the newest and most advanced method of authentication. Biometrics use physical or behavioral traits to verify the user's identity. Methods of biometric authentication include fingerprint, retina scans, voice analysis, or signature analysis. As each modality has its own strengths and weaknesses, it is important for financial institutions to know which method is best suited to meet their needs.

FINGERPRINT SCANS

VOICE BIOMETRICS

FACIAL BIOMETRICS AND RETINA SCANS

BEHAVORIAL BIOMETRICS

Fingerprint Scans

With the release of the iPhone 5s in 2013, scanning fingerprints has become one of the most common methods of biometric security. With the touch of a finger, the user can unlock their phone or sign-in to an account.

Fingerprints scanning is a quick and simple way for users to authenticate their identity. Juniper Research forecasts that more than 770 million biometric authentication applications will be downloaded every year by 2019, the majority of which will be fingerprint authentication due to the proliferation of smartphones.[5] With some government agencies now keeping databases of fingerprints, this method is increasingly relied upon as a secure method of authentication.

Though convenient, fingerprint authentication has a major flaw: once stolen or hacked, fingerprints are forever compromised. Such was the case in 2015, when hackers acquired the fingerprint data for 5.6 million federal employees.[6] The employees whose accounts were compromised will never again be able to use their fingerprints as a secure method of authentication.

Unfortunately, it's not that difficult to steal or copy a fingerprint. Some demonstrations have shown it can take less than five minutes for a potential thief to acquire a fingerprint and break into a device using seemingly innocuous items like gummy bears to create a mold.[7] Liveness testing could thwart some of these attacks but it requires expensive hardware an everyday user would not have access to.

[5] Juniper Research. https://www.juniperresearch.com/press/press-releases/biometric-authentication-app-downloads-to-reach-77
[6] TheGuardian.com. https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprint
[7] BiometricUpdate.com. http://www.biometricupdate.com/tag/gummy-bear-attack

Facial Biometrics and Retina Scans

Facial biometric software scans an image of a face, quantifies its features, and matches those features against stored templates in a database. Similarly, retina scanning compares the image of the user's eye to a template, matching the pattern of the retina. Both methods require a high-resolution camera in order to complete the scan.

In the era of the "selfie," facial and retina scans have received some recent attention. High security firms already make use of facial and retina scans. Furthermore, the only equipment the user needs is a camera.

Unfortunately, retina scans are open to some of the same weaknesses as fingerprint scans. There is no way for a user to change the pattern of their iris and, once a hacker acquires the data, it can never be used safely again.

Furthermore, liveness tests can easily be defeated by hackers. Researchers at the University of North Carolina found they could bypass facial biometrics by creating 3-D facial models using a few photos taken from a person's Facebook page.[8] The recently-released Samsung Galaxy S8, which has a facial biometric locking feature, proved susceptible to a similar hack.[9] Testers found that a simple still photograph will unlock the phone, leaving it vulnerable to hackers.[10]

While facial and retina scans may work well in controlled environments, using facial biometrics in the real world presents some challenges. Most cameras, especially on desktops or tablets, are not advanced enough to take the kind high-quality picture needed to complete a scan. Even with a proper high-resolution camera, environmental issues like lighting can foil facial biometric software.

A study at the University of Notre Dame found that the iris is susceptible to an aging process that "causes recognition performance to degrade slowly over time."[11] As the user ages, the pattern of their iris fades, creating a high level of false non-match error.[12] The same is true of facial recognition. As a person ages, their facial features change, making it difficult for the user to get a positive match with the database.

[8] Newsweek. "Facial Recognition can be tricked with Facebook photos." http://www.newsweek.com/facial-recognition-can-be-tricked-facebook-photos-492329/.

[9,10] USAToday. "Samsung S8 facial recognition feature fooled by photo, tester says." https://www.usatoday.com/story/tech/talkingtech/2017/03/31/photo-fools-samsung-s8-facial-recognition-feature/99889228/.

[11,12] Notre Dame. http://news.nd.edu/news/new-notre-dame-research-raises-questions-about-iris-recognition-systems/

Voice Biometrics

Voice biometrics use personal voice patterns to authenticate the speaker's identity. Qualities like the inflection of the user's voice are measured and tested by biometric software, which can then verify the identity of the user. There are two main methods of voice biometrics: vocal passphrases and passive voice biometrics. Vocal passphrases require the user to speak a specific passcode in order to be authenticated, while passive voice biometrics measure the inflection, pitch, and other qualities of the user's voice while they speak over the phone. With passive voice biometrics, no specific phrase or passcode is needed to authenticate.

Passive voice biometrics are especially convenient for the user. The biometric software measures the speaker's voice in the background of the call and does not require the speaker to remember a passcode.

However, this modality has serious restrictions. The user must make a phone call every time they need to be authenticated. Furthermore, voice biometrics require little-to-no background noise in order to positively confirm the identity of the speaker. This severely limits the number of locations that voice biometrics can be used successfully. Using a vocal passphrase in public is ill-advised, as anyone in the vicinity can hear the private passcode.

Voice biometrics can easily be stumped by every-day problems as well. Having a cold, being congested, or even lying down may change the user's voice and prevent a positive match. Furthermore, voice biometric security is easy to circumvent if hackers acquire a recording of the user's voice.

Behavioral Biometrics

Behavioral biometrics analyze user behavior to verify user identity by continuously collecting information about how the user interacts with a device. This modality can be applied in a number of ways. One example of behavioral biometrics is "gait recognition," which could be used to pair wearable devices by measuring the unique way a person walks as a method of authentication.[13] Another example is "phone use recognition," which measures the user's keystrokes on their smartphone and builds a profile based on a number of factors, such as how quickly the user types.[14]

Behavioral biometrics are extremely convenient for the user. There are no passwords to remember, no special equipment to buy, no environmental factors to consider. The user only needs to be themselves in order to authenticate their identity.

The major drawback with behavioral biometrics is that any small change in the way the user acts—a limp while walking or a hesitation while typing—can disrupt the biometrics and cause them to reject the user. As the user never knows exactly what typing speed or gait the behavioral biometric software is looking for, it can be impossible to correct any deviance in behavior and successfully login to an account.

Additionally, behavioral biometrics are only suited for particular environments. Gait recognition, for example, could never be used in an office setting—unless users were comfortable walking around in the middle of a meeting in order to unlock their devices!

[13] BiometricUpdate.com. http://www.biometricupdate.com/201701/wearables-could-use-gait-behavior-to-pair-with-other-devices
[14] Techradar.com. http://www.techradar.com/news/world-of-tech/future-tech/behavioural-biometrics-the-future-of-security-1302888/2

The Asignio Solution: 3-Factor Authentication

Asignio is a handwriting-based biometric authentication system. Unlike its competitors, Asignio biometric security uses all three authentication factors to create a layered security system that is both safe and easy to use.

Something You Know

Asignio users create their own "Asignio *Signature*," consisting of a set of characters or letters unique to them. Unlike a password or PIN, the user does not have to remember a long string of letters and numbers that change constantly. Asignio *Signatures* are personalized and unique, making them easy to create and easy to remember through muscle memory. In a study performed on Asignio test users, the users were asked to sign in to their accounts after five months of inactivity. All users were able to successfully login within three tries, without needing ask for assistance.

The Asignio *Signature* is much harder for a hacker to steal or copy than a simple password. With practice and muscle memory, users can sign-in with their *Signature* in under three seconds, making it difficult for a hacker to copy the movement. In fact, a recent Rutgers study found that logging in with a doodle or scrawl took two to six seconds less that typing in a password.[15] However, if a Signature ever becomes compromised, the user can quickly create a new one and continue to safely use their account.

Something You Have

With Asignio, the user's device is the physical token. Asignio's web-based, cross-device platform allows users to register a number of recognized devices. Asignio links the device and the user's account, making it impossible for someone else to login from an unregistered device.

Asignio takes security one step further by using the device's geo-location. By tracking where the user signs in, Asignio can quickly respond to any red flags raised by unusual activity.

[15] TheConversation. https://theconversation.com/could-a-doodle-replace-your-password-56792?xid=PS_smithsonian.

Something You Are

Asignio analyzes the way the user writes their personalized *Signature* to authenticate their identity. Asignio uses cutting-edge soft biometric technology to measure more than 25 unique aspects of a person's *Signature*. While most other handwriting biometrics only measure in 2-D, Asignio quantifies the *Signature*e along the X-and Y-planes, as well as measuring the time it takes the user to write their *Signature*. When the user signs-in, Asignio verifies their identity instantly through a detailed analysis of their Signature.

The False Acceptance Rate (FAR) for complex Asignio Signatures (a *Signature* with at least four strokes) is 1 in 2.3 million, making Asignio safer than other methods of biometric authentication. By comparison, the FAR of Apple's TouchID is only 1 in 50,000.

Additionally, Asignio uses behavioral testing to track how the user typically interacts with their accounts. If an account is somehow compromised, Asignio will flag the unusual activity and alert the user immediately, putting a stop to all fraudulent activity.

Asignio: Sign, Authenticate, Access

Asignio's 3-factor authentication verifies the user in under three seconds. The Asignio Signature and layered authentication system keeps the user secure every step of the way. With Asignio's web-based, cross-device platform, consumers and financial organizations can be secure in the knowledge that every sign-in is authenticated with the highest level of user validation.

Any account. Any device. One *Signature*.

Asignio