Voice Biometrics: Balancing Security, Usability and Privacy for User Authentication In Banking Applications and Mobile Payments

> "Billion dollar companies lose 3% or more of their revenues to mobile fraud"

Executive Summary

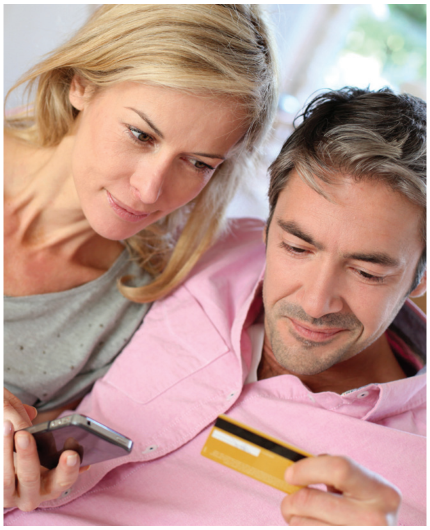
Organizations are losing millions of dollars every year to fraud, yet today, the only thing that can be done is to encourage the frequent, and impractical creation of increasingly complicated passwords that must be unique to every platform and service we use. Biometrics represent a new paradigm in user authentication – voice, fingerprint, iris – all unique to every user and therefore highly secure. Voice biometrics is the least intrusive of the biometric modalities and perhaps the most convenient element of a multi-factor authentication system where multiple modalities are used together. Text dependent or free speech modes provide ultimate flexibility and existing microphones in nearly all modern computing devices mean no additional hardware costs for the consumer. In addition, the ability to run voice authentication locally on the device, without a need to communicate with a server, afford a user complete control over their biometric credentials for unrivaled privacy. From social security organizations, to commercial call centers and mobile device manufacturers such as Apple and Samsung, biometrics are being rapidly adopted, and will inevitably become a necessary component of any system supporting remote, secure financial transactions.

Addressing the Need for Stronger Authentication

Traditional usernames and passwords used for identification and authentication assurance no longer suffice as an acceptable level of security to protect critical user information. Users, faced with dozens of online systems requiring increasingly stronger passwords to access their data, often revert to tactics that nullify the integrity of these stronger passwords by reusing the same password across many systems or failing to refresh them regularly. A recent report from mobile identity company TeleSign and RSA, the security division of EMC, surveyed 250 companies from a wide spectrum of industry verticals and found that they were losing an average of $92.3 million a year to mobile fraud. The average revenues of the companies in the survey were $2.5 billion, so these losses account for more than 3% of revenues – some organizations reported losing as much as 25% of revenues.

NECESSARY ATTRIBUTES OF STRONG AUTHENTICATION
Stronger authentication levels may be achieved by combining multiple identification and authentication factors:

- Something the user uniquely knows, such as a password
- Something the user uniquely has, such as a USB token
- Something inherent in the user's behavior, such as a frequent and consistent act
- Something physically unique to the user, namely a biometric characteristic like voice, fingerprint or iris



Value of Voice Biometrics for Strong Authentication

Voice biometrics authenticates a speaker based on numerous vocal characteristics including vocal tract geometry, harmonics, pitch and range. It offers an almost invisible authentication experience while providing a high degree of accuracy.

Security and Accuracy

Technical improvements in microphones and processing power in both mobile devices and servers, allows voice biometrics technology to offer more reliable, spoof-protected, accurate authentication, even in noisy environments. Enhanced voice capture capability and increased computational processing power enable more sophisticated algorithms to be implemented in the authentication process. As a result, spoofing and hacking protection mechanisms can be implemented to ensure systems are protected against replay attacks and unauthorized access to the user's biometrics credentials.

Convenience

Voice biometrics is the least intrusive of all biometric modalities used for authentication. Voice authentication can be implemented with a one or two-second text-dependent (fixed) passphrase or with two to three-second, text-independent free speech that will validate a user's identity. In the latter case, the authentication is completely passive to the speaker providing the highest level of convenience.

> "Voice biometrics offer the highest levels of security, convenience and privacy"

The two modes provide an option to balance convenience with the level of security risk required. For example, a bank presented with an online transaction amount under $1,000 may require a lower level of confidence to authenticate than a transaction that is equal to, or more than $10,000. The applicable parameters may be adjusted according to specific level of risk requirements.

Cost

Voice biometrics is a more cost-effective method of authentication than other biometric modalities, as it does not require any hardware investment by the user. Existing microphones in mobile phones, tablets or PCs and in many other consumer electronic devices, eliminates this need and any additional associated costs.

Privacy

Voice biometrics provides server-based or device-based application deployment options. Server-based authentication engines running on-premises provide control over service and data storage by the payment service provider. When running locally on an embedded device, users maintain control over their own biometric credentials, thus better protecting privacy by eliminating the need to communicate with servers. User privacy is a critical differentiating feature for future online and Internet of Things (IoT) applications.

Use Cases

Proof of Life – Beneficiary Payments

The South Africa Social Security Agency (SASSA) engaged AGNITiO partner, NET1, to deploy their Voice iD authentication engine to revolutionize the in-person "proof of life" verifications, where citizens historically had to visit their nearest social security office to prove they are still eligible for social security benefits. The system was rife with challenges – it was time consuming, transaction costs were high, fraud was common and it was a significant physical burden on the elderly and physically handicapped who were being asked to travel great distances.

Today, citizens can simply call in to perform the same task with their new biometrics-based grant payment disbursement system that rolled out to over 10 million beneficiaries. The program has already resulted in a savings of $200 million by removing 650,000 recipients from the register and close to a 50% reduction in cost per transaction. More importantly, the new program has delivered a dramatically improved quality of life for South African citizens who no longer need to endure long journeys to stand in longqueues to prove their eligibility for benefits.

Online Fraud Detection

As the online fraud detection market continues to try to keep pace with the rapid expansion of and advances in cybercrime, telephony-based voice authentication technology combined with passive biometric analysis is being used to reduce online fraud. According to a 2014 Gartner report by Avivah Litan on telephony fraud, large financial services institutions report that about 30% of their fraud occurs via compromises in multiple channels including the telephony channel.

In this market, biometric analysis is done "behind the scenes", transparent to the user as there are no enrollment requirements. Over time, the system is trained on a user's biometric "signature" so that it can compare the signature to known fraudsters, or monitor the legitimate user's behavior in order to determine whether or not they are being impersonated.

> "Over 10 million enrolled in one deployment to authenticate, fight fraud and reduce costs"

Two of the leading companies in this area of fraud detection - Verint and Pindrop - use AGNITiO's KIVOX Passive Detection engine to reduce this type of online fraud. Their solutions identify and authenticate callers as they speak real time, passively screening all incoming calls against a blacklist of known fraudsters. Between 75% and 95% of the cases detected are repeated attacks, so solutions that are able to identify professional fraudsters can have a tremendous impact, reducing fraud by 75% in just months after deployment, according to customer data.

Mobile Payments and Multifactor Authentication

Apple and Samsung recently entered the mobile payment market with their own approach to balance security, convenience and privacy for their users. Apple uses fingerprint biometrics and Near Field Communications (NFC) technologies to authenticate users for payment transactions providing more secure and convenient online payments. Samsung launched its Galaxy S5 with a PayPal solution that allows mobile PayPal transactions using the device's fingerprint sensor and that also follows a FIDO (Fast IDentity Online) model.

The FIDO Alliance was founded with the mission to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services including mobile payments. It is expected that other mobile device manufacturers and online payment providers will also accept and integrate various biometrics modalities under these models.

Conclusion

The future of strong authentication for online and mobile payments will be based on the multi-factor paradigm, integrating multiple biometrics technologies that will co-exist to enhance security and convenience. Users and services will have choices among which and how many modalities to use on their own or in combination, depending on the risk of the operation for a particular application. Voice biometrics technology is ideal in a multi-factor approach as it strikes the balance between authentication accuracy, security and usability. The entire AGNITiO KIVOX suite of voice biometrics products is designed to comply with the broad requirements of strong authentication in the payments ecosystem.

> “The strongest authentication for online and mobile payments will be based on the multi-factor paradigm”

KIVOX Mobile

The FIDO Ready™ KIVOX Mobile SDK is available for implementation within the mobile and payment ecosystems for on-device secure speaker verification and in authentication applications for smartphones and other embedded platforms. Enrollment and matching are done locally. There is no need for network connections or voice transmissions.

KIVOX 360

The KIVOX 360 authentication server provides the most advanced speaker authentication capabilities available enabling mobile, web, desktop and IVR voice applications to verify the identity of individuals in a highly secure, automatic and effortless manner. Optimized for fixed passphrase implementations, KIVOX 360 creates a unique biometric voiceprint (BVP) used for subsequent authentication in any channel and with only a single enrollment. It delivers a successful identification rate of more than 99.5%, with a false acceptance rate of less than 0.1%. With its patented anti-spoofing technology, KIVOX 360 detects up to 97% of replay attacks, as well as many other spoofing attacks such as cut-and-paste.

KIVOX Passive Detection

Designed for call centers, KIVOX Passive Detection uses natural speech for caller identification. Previously recorded calls are used to create a BVP. By comparing these BVPs with the voice used in subsequent calls, a person’s identity can be verified in a fully transparent manner without the need of any active enrollment.