SayPay TECHNOLOGIES, INC.

Nine Use Cases for Voice Biometrics

More companies than ever are turning to voice biometrics. With its ability to combine convenience and security, some traditional and a growing number of applications are tapping into its unique, hands-free potential. In this article, we explore voice authentication trends and creative approaches that are moving voice deployments in new, radical directions.

Education

Is the person taking that online exam who they claim to be? Self-service testing provides flexibility and cost efficiencies, but educators who conduct testing online are highly susceptible to identity abuse. Possible voice authentication uses for overcoming this problem include driver education, professional certifications, and online colleges. Online driver training school, Aceable of Austin TX, recently added voice authentication for positively identifying students through their mobile app. Because voice is impossible to imitate, is fast, and works on any smartphone or tablet, it is an ideal biometric authentication option. Implementations are most effective when deploying voice verification at random times during testing, as well as device identification for multi-factor authentication.

Enterprise

Many companies rely on cumbersome and expensive hardware tokens/fobs to improve security for physical access. Some even issue cards with embedded chips in additional to a stand-alone card reader. These solutions display a numeric value that changes every minute, or require a challenge-response method including the entry of a PIN to generate a value for host authentication. The result is always the same: expensive to deploy and support, tedious to use, and detested by users. Mobile-based soft-token substitutes eliminate the extra hardware but carry all of the other shortcomings.

Data security provider Vasco have been an innovator in offering multi-factor solutions to their hundreds of clients. An early adopter to biometrics, Vasco offers fingerprint and facial scanning to its suite of identity options and is appraising voice. Voice-based enterprise access requires no additional hardware, no PINs or passwords, and extends security from two- to three-factors when using a unique user or session value.

Other enterprise applications where voice is being deployed include systems supporting voice mail, secure room access, employee password resets and for time and attendance tracking.

IoT

An estimated 20+ billion devices will be online by 2020, with most of them being enterprise-connected. The task of securely locking down a countless number of a company's devices, and the data storage systems to which they connect, is the nightmare to every CSO.

In its TechRadar™ Internet of Things Q1 '16 report, Forrester claims that the explosion in IoT has paid little thought to security. In a famous device breach in 2012, hackers took control of cameras on PCs, baby monitors and security devices through unprotected passwords. The result was significant brand damage to the vendor and costly monetary penalties. Small- and medium-sized companies will no longer be able to rely on password protection for system and device access. Fortunately, voice biometrics can be deployed on every phone that has a microphone, offering the highest form of user authentication.

Automobiles

Have you ever considered why you need to call a locksmith when you lock your keys in your car? Shouldn't you be able to unlock your vehicle with your phone, providing you can prove your identity? Some auto manufacturers are outfitting vehicles with the ability to unlock the vehicle using an NFC-embedded card or phone. Next step, connected cars can be unlocked and driven without a key. The user will simply access the vehicle from a phone app by speaking a code or passphrase. Once inside, the user may use the hands-free voice acceptance device. User controls for setting restrictions on auto speed and location will assist parents with teenage drivers, secured of course, by the parent's voice biometric.

The automotive industry may have the most to gain from the hands-free convenience and security of voice solutions. Hands-on-the-wheel at all times eliminates hands and fingers as input devices. Fortunately, advancements in voice sciences means drivers can be productive while behind the wheel with their online connected cars and devices.

For more information, check out the report by Markets and Research, "Advances in Automotive Voice Recognition Market" that presents an analysis of voice recognition growth potential in various automotive market segments.

Identity Protection

Ironically, the same companies whom consumers and businesses trust to monitor and protect their identities offer nothing more than password-based access security. I recently conducted an experiment by changing my password and contact details with the identity protection service that I use. I received an email notifying me of the change, but only at the *new* email address that I had registered. And no text alert whatsoever.

As with other websites that contain confidential consumer information, identity protection services need to hold themselves to a higher access security standard. Their roadmap needs to include integrating voice-based authentication solutions whether deployed on a mobile app, through PC-based voice acceptance means, or outbound phone calls with biometric IVR services.

Financial Services

Financial institutions have been early adopters of voice biometrics with dozens of deployments announced in the past 18 months. Banks using voice authentication in their call centers have slashed costs by reducing fraud and agent call times, and have improved the customer experience. Now, call centers across all industries are signing up as well. Banks and brokerage houses have also stepped up to offer bank sign-in using voice, including most recently big names like HSBC, Schwab and TD Waterhouse.

For those lagging, regulators will hold every financial services company accountable for the slow pace in which they have moved to improve account access security. While out-of-band authentication via text is a common practice, its easy-to-exploit vulnerabilities were denounced by the NIST in August 2016. Voice biometrics offer financial services a secure and convenient solution available to everyone who owns a smartphone—so these days, practically everybody.

Website Access

The bane of every internet user is remembering a unique password for every unique website. The impact has been softened with the ability for browsers like Chrome to remember your username and password—however, this creates a serious security exposure if your PC is ever lost, stolen, hacked or infected. New federated single sign-on models like OpenID Connect provide some relief for websites that don't hold highly confidential personal data. However, accessing high-security websites that provide financial, health and identity protection are not candidates for this option.

Voice biometrics provide a ubiquitous alternative where higher security is essential. For these environments, the user simply speaks a passphrase, or preferably a one-time password code, into their mobile phone or PC on the sign in page. The on-premise or cloud-based server then verifies the user against their voiceprint. At a time when such high importance is placed on customer experience and protecting consumer identities, adding voice authentication could be a key differentiator in growing acquisitions, reducing attrition, and dramatically improving access security.

Smart Home

When I arrive home with my arms full of groceries, I would very much value being able to unlock the door without fumbling for keys. I look forward to the day that I can just speak a passphrase like "Hello Smart Home" or my street number and then hear the deadbolt disengage. In addition, my home security system would deactivate simultaneously. When I go to bed, my security phase may be, "Smart Home, lock up." All of the door locks would engage and the window sensors become activated.

The recent study "Securing a Smart Home Network using Voice Biometric" proposes voice as the choice for authentication above all other biometrics for its hands-free, frictionless user identity capabilities.

Embedded Devices

Those familiar with voice biometrics know that voice authentication must be processed online to meet high-quality, high-security standards. Solutions deployed locally on smartphones are incapable of meeting the precision only possible in online voice processing systems. Online voice authentication performs intensive sound spectrum analysis for each authentication request using a complex formula of various algorithms. Local authentication generally has very high "false-accept" rates making it applicable only for light-weight, low-security needs. However, as IoT grows and more components are connected online, the capability of integrating embedded devices in homes, automobiles, and the workplace becomes another opportunity for voice authentication.

Summary

We believe consumers will be soon able to securely check their bank balances, access their office voicemail, and refill a prescription as they are dressing for work, driving their cars, or getting ready for bed. Industries across the map are beginning to recognize the combined convenience and security of voice authentication. At SayPay, we encourage companies in all industries to consider how each person's unique voice is a safe and convenient replacement for hardware tokens, passwords, or keys. To learn more about voice biometrics, please download our whitepaper at www.saypaytechnologies.com.

Steve Hoffman is a published thought-leader on biometric authentication and the CEO of SayPay Technologies. He can be reached at steve@saypaytechnologies.com.