Talking passwords: voice biometrics for data access and security

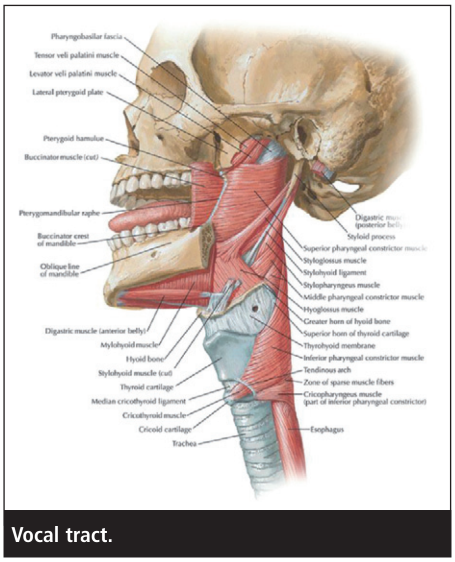
Mikhail Khitrov

Mikhail Khitrov, Speech Technology Center

Among the five innovations listed in IBM's 2011 five-year forecast was the biometric key. "You'll never need a password again," say IBM experts, referring to the fact that biometric features, including voice, face, fingerprints and retina, are absolutely unique to every individual.

In this article, we focus on one of these biometric technologies, voice, and consider the use of biometric voice identification and verification as a password for accessing devices and information.

Is it enough to use one's voice for data and device security, or should voice biometrics be combined with other methods to achieve even higher levels of security? Is it safe to say we can go ahead and 'forget' all our passwords, once and for all?

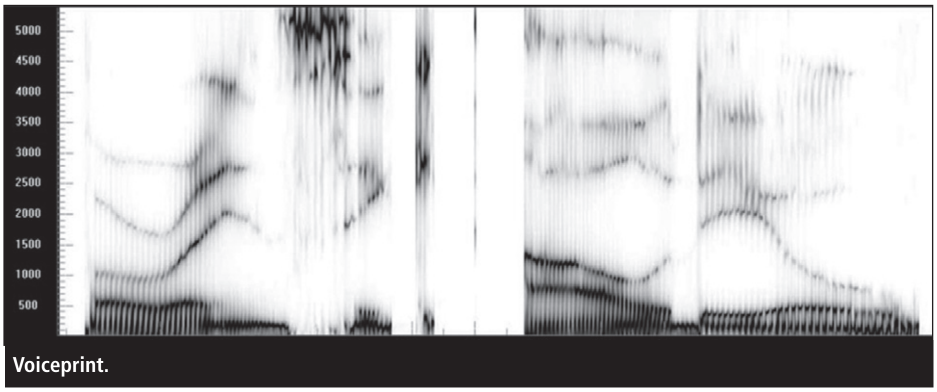

Pharyngobasilar fascia
Tensor veli palatini muscle
Levator veli palatini muscle
Lateral pterygoid plate
Pterygoid hamulue
Buccinator muscle (cut)
Pterygomandibular raphe
Buccinator crest of mandible
Oblique line of mandible
Digastric muscle (anterior belly)
Mylohyoid muscle
Hyoid bone
Stylohyoid muscle (cut)
Thyroid cartilage
Median cricothyroid ligament
Cricothyroid muscle
Cricoid cartilage
Trachea
Digastric muscle (posterior belly)
Styloid process
Superior pharyngeal constrictor muscle
Styloglossus muscle
Stylohyoid ligament
Stylopharyngeus muscle
Middle pharyngeal constrictor muscle
Hyoglossus muscle
Greater horn of hyoid bone
Superior horn of thyroid cartilage
Thyrohyoid membrane
Inferior pharyngeal constrictor muscle
Tendinous arch
Zone of sparse muscle fibers
Cricopharyngeus muscle (part of inferior pharyngeal constrictor)
Esophagus

Vocal tract.

First, let's make it clear that biometric technologies used in information security, whether for voice, face, or other modality, do not rely on passwords and PIN codes. Passwords and PIN codes can be discovered, acquired and used by individuals other than those originally authorising those codes. Biometric technologies do not rely on what you know, or what you possess, but rely on what you are.

This is what makes biometric passwords considerably more secure than PINs; they are indistinguishable and indivisible from the person using them. The irreducible uniqueness of the human voice makes it stand out from a security perspective even in contrast to other biometric features.

Voice biometrics, also referred to as speaker recognition, is a technology that identifies and verifies a person on the basis of his or her unique voice characteristics. Several physiological features contribute to this uniqueness of voice, including the structure of the vocal chords, the trachea, the nose, the placement of teeth, as well as the way a person accentuates sounds. In combination, such characteristics are as individual as fingerprints and cannot be falsified or transferred.



Voiceprint.

Contactless

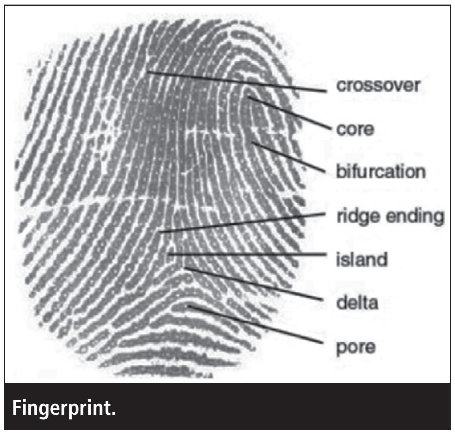
The feature that really distinguishes voice biometrics from other modalities is its contactless application. Unlike fingerprints, voiceprints can be taken remotely. With voice, there is no need to be in physical proximity to the print capture device, as there is with fingerprinting and vein recognition. This means voice biometrics can be used widely, and in a great many more situations, for example, while driving, from another room or even via mobile devices.

The main principle behind any voice biometric system is this: the user or caller utters a passphrase that is captured by the system that is then matched against a previously stored voiceprint. The matching procedure generates a score representing how accurately the new utterance matches the stored voiceprint. Access score thresholds can be pre-set for enhanced security. For instance, if a match procedure generates a low score, match access will be blocked.

One more reason to trust voice biometrics as a passkey technology is its simplicity; after all, we speak all the time. With voice biometrics, a person only needs to do what comes naturally to confirm his or her identity, for instance, say his or her name, telephone number or repeat a prompted phrase.

It's simple from a technical and market perspective as well, as voice is easily delivered: most modern devices already have built-in microphones, the primary hardware component needed for voice identification.

According to the most recent Unisys survey on what biometric technologies consumers prefer, voice biometrics comes first; 32% of respondents said 'yes' to voice recognition. Voice biometrics are easily implementable as a passkey in various spheres: in mobile banking, in accessing personal devices and logging in to social networks. An added convenience is that voice biometrics can be run on a remote server, 'in the cloud' and not on the user's own device. In this case, even if a device is lost,



Fingerprint.

stolen or misplaced, the unique voice characteristics associated with it are not lost, stolen or otherwise compromised.

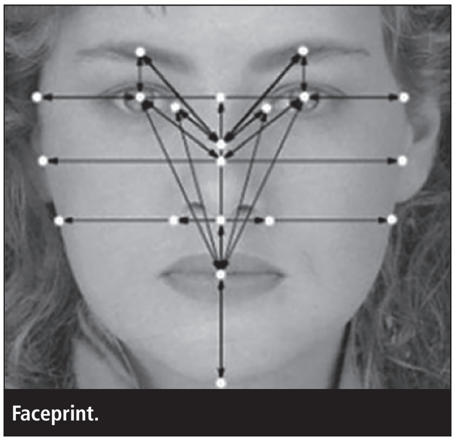
Many people wonder about the relationship between language and voice biometrics. It should be emphasised that the world's incredible linguistic diversity does not place any limits on voiceprint technology. Speaker accent, language and dialect do not play a role in speaker identification and verification carried out using automated voice-based methods.

Most of us are familiar with the kind of speech recognition used in today's smartphones. We can ask questions out loud and get answers 'hands-free'. Such speech technology applications are language-dependent, and you generally need to know English to use them, making them inaccessible to entire populations. Using voice as a password technology, however, is language independent. It can be installed on any device and implemented and used worldwide.

Challenges

Despite all the benefits of using voice as a password technology, there are still some challenges ahead for voice biometrics. First, the technology cannot guarantee 100% correct identification, though neither can any of the other biometric modalities. At a more practical level, the following are more basic reasons that result in errors in speaker identification:

- environmental noise, which varies as to noise type and noise level
- presentation effects, including speech sample duration, the psychophysiological state of the speaker (eg illness, emotions), effects of vocal strain
- channel effects, including interference) and distortion (eg frequency response, channel encoding)



Faceprint.

Supplementing voice biometrics with other biometric modalities brings us closer to 100% correct identification and authentication. Multibiometrics and multifactor authentication represent today's solution to less-than-perfect results achieved by any single technology, raising the level of security by combining two biometrics modalities, for instance, voice biometrics with face or fingerprint recognition. For example, if a device first asks for your fingerprint and then asks you to repeat a combination of numbers aloud, there is zero chance that an unauthorised person will be able to access your device.

Multifactor authentication as a passkey combines 'something you are' with 'something you have'. The combination cannot be guessed or otherwise attained. The 'something you are' means biometric identifiers that are unique to you, while the 'something you have' means a key, a USB token, something in your physical possession. If the 'something you have' is stolen, it will be inaccessible without the second part—the 'something you are'.

Of course, a voice cannot be stolen, and even recordings of voices cannot be used to fool automated voice biometrics systems. Multifactor authentication makes voice as a password technology extremely reliable.

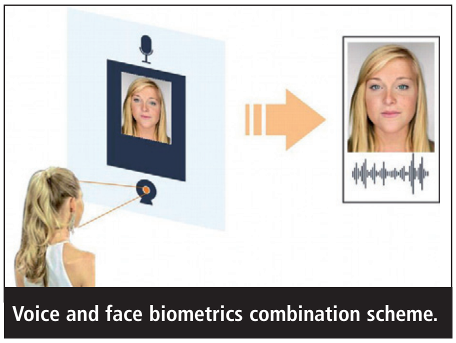
Gartner analysts have recently recommended that businesses use a combination of authentication methods to enhance security, including voice biometrics. They reportedly expect at least one major financial institution to implement voice -based caller authentication by 2013.

Applications

Should these recommendations be heeded, there are several domains and ways in which voice biometrics can be used to ensure secure and convenient user authentication:

Call centres and IVRs

Customers interact with IVRs (interactive voice response systems) for numerous reasons, for instance, to get bank account balances, medical test results and to track orders. These interactions are all about gaining access to sensitive information. What customers have in common across these cases is a desire to access this private information quickly and securely.

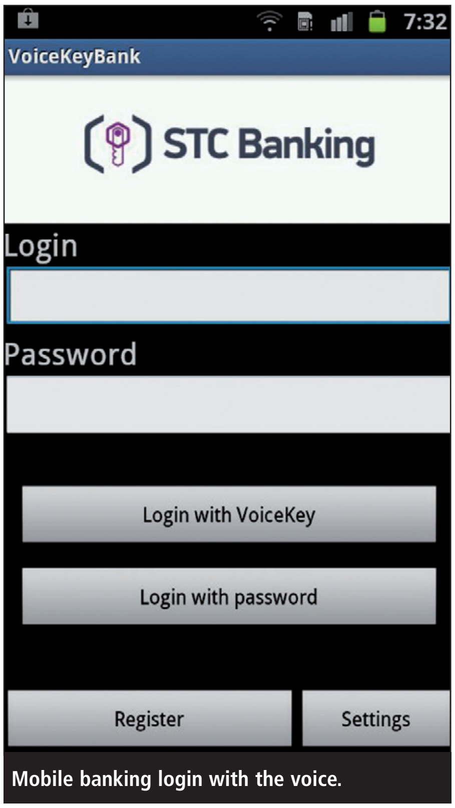


Voice and face biometrics combination scheme.

With current security measures, it takes a long time for callers to get the information they need over the phone, and call centre agents waste their time working to identify callers, instead of working to get them the information they seek. When IVRs or call centres use voice authentication, neither the caller nor the agent wastes much time with identity confirmation and can get down to the issue of dealing with the caller's immediate service requests.

Mobile voice-based authentication

Because we use our smart devices for so many things, as personal notebooks, as photo and video albums, as mobile gateways for banking and other commercial applications,



Mobile banking login with the voice.

they are the storehouse of much of our most sensitive information and any of it can be compromised if the device is lost, stolen or otherwise compromised. Voice-based authentication helps protect personal information stored on smart devices as only authorised persons can gain access to data stored on the device.

Cloud computing and BYOD

Moreover, as employees tend to prefer their personal smart devices to access enterprise resources, sometimes called the BYOD, or bring your own device, phenomenon, IT departments have to invent new policies and procedures for enterprise data protection.

Users increasingly rely on smartphones and tablets for work, and recent research shows that these more mobile workers are putting in longer hours. Modern organisations are taking advantage of this trend by making it easier for their employees to connect to enterprise resources. That not only means giving employees resource access from remote locations, but also providing a consistent end user experience whether the employee is working from home, from a hotel or from the airport.

> ***"Voice signature over the phone (in IVRs and call centres) offers a natural, convenient and legally binding alternative to hand-written signatures"***

This trend threatens to reduce control over enterprise computing, as it increases the probability of theft of important corporate information through employees' personal devices. For most IT professionals, the combination of cloud computing and the BYOD trend means security has changed forever. IT departments face greater pressure, as the need to protect corporate data explodes across a number of devices and platforms, and the need to manage, monitor and support them all remains constant.

Enterprises have to choose whether to limit this newfound flexibility and productivity by prohibiting the use of personal devices in the office, or to find a secure and user-friendly way to authorise employees to use cloud and BYOD resources for work. Analysts predict that 90% of organisations over the next two years will support enterprise applications on employees' personal devices. It is clear that enterprises need to adapt existing corporate IT infrastructures to emerging trends. Voice-based authentication in such cases can be used as an effective security method.

Voice e-signatures

Voice signature over the phone (in IVRs and call centres) offers a natural, convenient and legally binding alternative to hand-written signatures, for example, on health insurance applications, financial documents and a range of other e-communications needing personal authorisation.

Voice biometric technology can also be deployed to access social network accounts, email accounts and other platform logins.

Social networking and voice biometrics

As social networking is adopted in more domains, social network platforms are becoming storehouses of confidential professional and corporate information and such networks can also be targeted by cyber-criminals. Voice biometrics may enhance security, by adding biometric passwords to account logins on platforms such as LinkedIn and Facebook.

Conclusion

Given the pros and cons of using voice biometrics as a password technology, it is clear that it is generally useful in a range of spheres. Combining it with other secure technologies means added trust and reliability. While voice biometrics might appear to be a complex solution for data security and access, experts agree that biometrics technology will soon become part of our everyday lives. The examples above attest to the need for voice biometric passwords; we just need a bit of patience to see these developments come to life.

Resources

- Bring-Your-Own-Device. http://en.wikipedia.org/wiki/Bring_your_own_device. Accessed January 2013.

References

- IBM 5 in 5 forecast 2011. http://www-03.ibm.com/press/us/en/pressrelease/36290.wss. Accessed January 2013.
- Voice Biometric Authentication Best Practices: Overcoming Obstacles to Adoption, 2012, Opus Research. http://opusresearch.net/wordpress/2012/01/17/research-report-voice-biometric-authentication-best-practices-overcoming-obstacles-to-adoption. Accessed January 2013.
- Scheips, D. 'Voice recognition – benefits and challenges of this biometric application for access control'. http://www.sourcesecurity.com/news/articles/co-3108-ga.4100.html. Accessed January 2013.

About the author

Mikhail Khitrov founded Speech Technology Center (STC) in the early 1990s, in St. Petersburg, Russia. Today, STC is a global provider of innovative systems in high-quality recording, audio and video processing and analysis, speech synthesis and recognition, and real-time, high-accuracy voice and facial biometrics solutions. STC innovations are used in both public and commercial sectors, from small expert laboratories, to large, distributed contact centres, to nation-wide security systems. STC recently developed VoiceKey, a voice authentication technology for data security, which is already being used as application for secure logon to tablets and iPads. The company is currently working on VoiceKey adaptations for banks; to manage such services as account balance queries and automated client approval/disapproval lists. For more on STC, visit the company website at www.speechpro.com.