Voice biometrics: success stories, success factors and what's next

Brett Beranek

Brett Beranek, Nuance Communications

An increasing number of organisations use voice biometrics for internal or customer-facing authentication. In 2010, Opus Research said, "With over five million registered voiceprints supporting user authentication around the globe, it appears that voice biometric-based solutions are poised to assume the pivotal role of user authentication to support higher levels of trust among users of mobile apps, remote monitoring, distance learning, e-medicine, e- government and a host of other social activities or transactions."

A year later, the number of voiceprints had increased to 6.5m. Today, Nuance customer organisations alone have amassed more than 30m voiceprints – one more sign of how quickly and widely voice biometrics are being accepted.

Barclays, T-Mobile, Vanguard, Vodafone and ANB are among the merchants, telcos, banks, government agencies and other consumer-facing organisations that have implemented voice biometrics to improve their customer service experience.

Voice biometrics enables these organisations to reduce or eliminate the need for PINs, passwords and other common authentication methods, as well as the interrogation-style Q&A that comes when customers forget passwords.

Consumer frustration

Opus Research summed up what recent research and other companies shows: "You get a picture of a frustrated set of consumers ready to take advantage of new technologies that reduce the time it takes to carry out their business both over the phone and online."

More specifically, the research found that 85% of people are dissatisfied with current authentication methods and that 90% of people are eager to use voice biometric solutions in place of traditional methods of authentication if it means the same high levels of security.

There's another reason why voice biometrics deployments are growing at a healthy clip. The technology is an opportunity for organisations to save and make money. Some of the savings comes from increased automation, which means lower contact centre overhead costs. By making the authentication process fast and frustration-free, voice biometrics also frees up time and caller patience to listen to upselling pitches.

A US cable services provider reported over $4m in annual operational savings alone. In addition, one of Europe's largest telecommunication providers reported the financial benefits resulting from improved customer loyalty and new acquisition far surpassed the $2m in actual annual operational savings they realised.

Fraud reduction

Voice biometrics is effective at reducing fraud. One of the top three US financial institutions used voice biometrics to uncover fraud groups and fraud patterns that it wasn't aware of, allowing the organisation to implement mitigating measures to significantly reduce fraud throughout the organisation. An Israeli bank experienced a ten-fold reduction in fraud following the deployment of voice biometrics.

Beyond improving the customer experience in service channels, reducing operating costs and increasing revenues, and dramatically reducing fraud, voice biometrics also creates opportunities for merchants, telcos, banks, government agencies and other consumer-facing organizations to accommodate and even leverage a variety of trends to their advantage. These trends include the 100% mobile phone penetration in most developed and many developing countries and a growing consumer preference for self-service options when interacting with customer service.

Voice apps

Siri, Google Now, Samsung S Voice and other speech-controlled personal assistants are conditioning consumers to feel comfortable asking their phone for information. Companies that have mobile customer service apps can leverage that familiarity by speech-enabling them.

Over the past few months, US firms USAA and Geico have both deployed Nuance's voice assistant technology in their mobile apps. USAA offers insurance, banking, investment and retirement products and services to more than 9.4m members of the US military and their families. Insurance company Geico now offers Lily, an interactive voice assistant, on its mobile app.

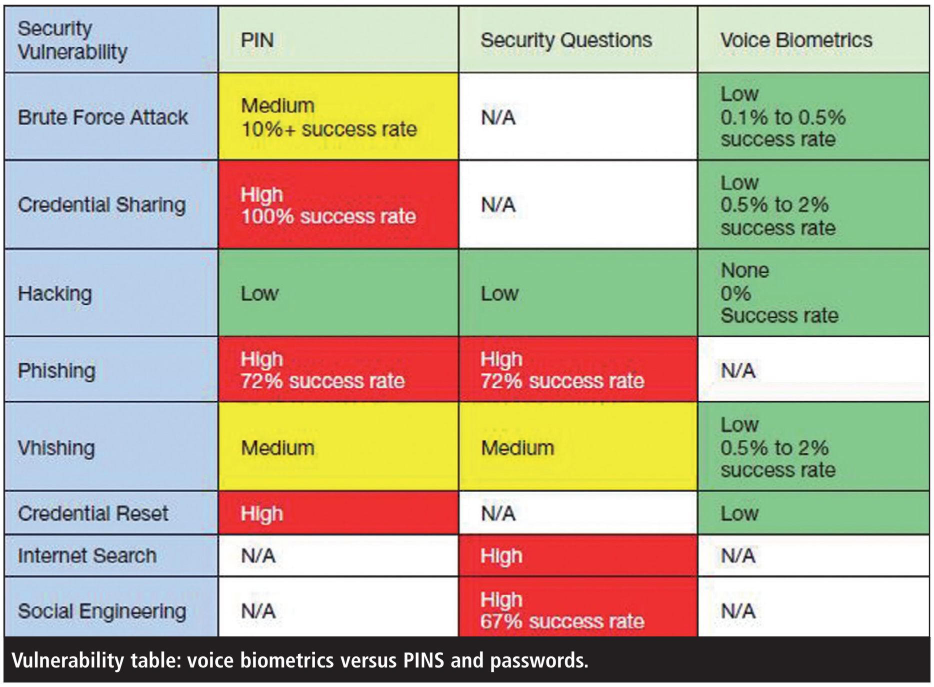
By extending voice biometrics out to their apps, companies free customers from the hassle of typing PINs, passwords and other log-in information. This isn't a minor benefit, either. Nuance surveys found that 67% of mobile users have to reset a PIN or password at least once a month. 96% said they make mistakes while typing log-in information.

There's another potential, less obvious benefit. Customers whose mobile phone is their primary or only way to get online might choose less complex passwords – such as no numbers or capital letters – to reduce the chance that their log in will fail due to a typo. That choice increases the possibility that their account will be hacked, which incurs a variety of costs for the company where they are a customer.

Finally, for customers who are walking on a busy pavement, or driving, the ability to prove their identity simply by speaking has safety benefits, too. Companies could highlight that aspect in their app's marketing to encourage adoption.

About 76% of consumer respondents in a recent survey said they find self-service more convenient than other channels. This preference is even higher among Gen Y consumers at 82%.

The cost of adding voice biometrics to an IVR is incremental, so supporting this preference doesn't have to be expensive. For customers who prefer speaking with an agent, voice biometrics improves that experience, by eliminating the need for any overt authentication process. There is no longer a need for agents to interrogate callers, which helps them foster a positive relationship with callers.



Security Vulnerability	PIN	Security Questions	Voice Biometrics
Brute Force Attack	Medium 10%+ success rate	N/A	Low 0.1% to 0.5% success rate
Credential Sharing	High 100% success rate	N/A	Low 0.5% to 2% success rate
Hacking	Low	Low	None 0% Success rate
Phishing	High 72% success rate	High 72% success rate	N/A
Vhishing	Medium	Medium	Low 0.5% to 2% success rate
Credential Reset	High	N/A	Low
Internet Search	N/A	High	N/A
Social Engineering	N/A	High 67% success rate	N/A

Vulnerability table: voice biometrics versus PINS and passwords.

Voice biometrics also can enable self-service PIN and password resets. Some real-world deployments have achieved self-service rates of 99%. For consumer-facing applications, that high automation saves money by reducing contact centre staff levels and frees agents to provide better service. For internal enterprise applications such as IT helpdesks, high automation can mean that support staff can be retasked to revenue-generation projects.

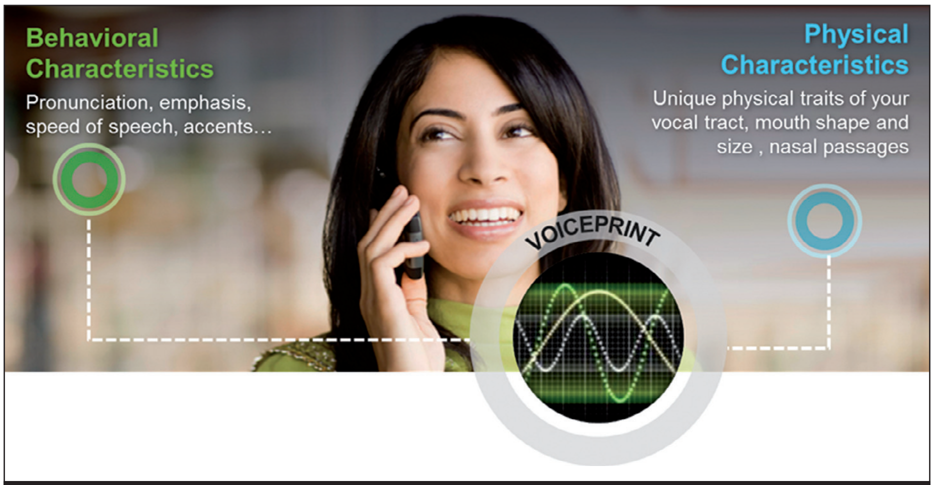
Financial services

In financial services, banks and other institutions can use voice biometrics to comply with Federal Financial Institutions Examination Council (FFIEC) requirements for two-factor authentication.

Voice biometrics eliminates the cost of providing and supporting two-factor authentication devices such as key fobs, as well as the security risks and replacement costs when they're lost or stolen. Voice biometrics also provide an opportunity to capture the voices of fraudsters for prosecution and to build a database of known fraudsters.

> ***"Voice biometrics also provide an opportunity to capture the voices of fraudsters for prosecution and to build a database of known fraudsters"***

For banks and brokerages that cater to high wealth individuals, voice biometrics eliminates the traditional Q&A of PINs, passwords and mother's maiden names, a procedure that customers find annoying. Voice biometrics – whether in the form of passive or active authentication – helps those firms provide the annoyance-free, white-glove service that's key for retaining high value customers.



Behavioral Characteristics
Pronunciation, emphasis, speed of speech, accents…
Physical Characteristics
Unique physical traits of your vocal tract, mouth shape and size , nasal passages
VOICEPRINT

Enabling high accuracy with text-independent voice biometrics and very short utterances is likely to become achievable very soon.

For example, Barclays uses voice biometrics to automate the identification and verification process used in its contact centres. Through passive voice biometrics, the organisation has improved service and reduced call times by 5%. 95% of callers who use the voice authentication are successfully verified and 93% have given Barclays a 9 out of 10 satisfaction rating.

Many financial institutions say they struggle to get PIN-based self-authentication rates above 55%. That means the remaining callers have to endure an average of 60 seconds' worth of live interrogation, which costs the financial institution money in the form of contact centre staff resource. The Q&A process also is stressful for agents, who deal with annoyed customers by rushing to resolve their issue and skipping upsale pitches.

Nobody wins in that scenario, but unfortunately it's the norm. Because it's so common, it's also an opportunity for financial institutions to use voice biometrics to provide a level of customer care so convenient that their brand stands out from the pack.

After implementing voice biometrics in its IVR, one global bank reported an automated authentication rate of 95%. Customers who bypass or fail automated authentication also now avoid a Q&A because they're passively authenticated while speaking with the agent.

As a result, call-handling time was reduced by 20 seconds, while time spent upselling increased by 40 seconds. The combination of automation-related savings and increased upsale revenue paid for the voice biometrics investment within six months. The bank also got an unexpected benefit of reduced agent turnover due to lower stress.

Telecom services

Turkcell is Turkey's largest mobile operator. Its customers account for about 40% of all registered voiceprints worldwide, so it's worth studying for insights into how telecom providers and other organisations can educate consumers about the benefits of voice biometrics.

Turkcell created a TV commercial to build awareness of 'Voice Signature', which reduced authentication to 5 seconds, that is a 20-second reduction for Turkcell's consumer customers and 40 seconds less for its corporate subscribers. Before the commercial began airing, about 1.5m customers had enrolled in Voice Signature. Afterward, another 2.5m signed up.

By the end of 2011, customers had used Voice Signature to authenticate themselves more than 11m times. That runaway success highlights another thing organisations should look for when comparing voice biometrics solutions: the ability to scale quickly and cost effectively.

"Customers like the very simple and fast authentication process of only 5 seconds," says Fahri Arkan, assistant general manager of information technologies at Global Bilgi, which provides CRM for Turkcell. "As a pioneer service in Turkey, we first launched this system for a limited number of subscribers, but it attracted more attention than we had expected and reached 2m users in a short time."

Voice Signature provides Turkcell with a reputation for great customer service. That's a helpful market differentiator in an industry as hypercompetitive as mobile, and for just about every other vertical, too.

Considerations

As the voice biometrics market grows, so does the range of vendor solutions. That expansion means organisations have to be savvy about features. Besides the solution's scalability and the vendor's reputation, organisations also should look for:

- Algorithms that are sophisticated enough to work around problems such as crosstalk and background noise. That intelligence minimises the chance that callers will have to repeat themselves.
- Anti-spoofing safeguards. One example is playback detection algorithms, which determine whether the caller's speech is unnaturally similar to a past voice utterance from the legitimate user, indicating an attack by a malicious individual that is playing an audio recording. Another example is liveness detection, which detects is a change in speaker has occurred following the authentication process, also indicating a playback recording attack.
- Automated fraudster detection. Sophisticated voice biometric solutions can automatically build fraudster databases and detect malicious individuals as they interact with a smartphone, IVR or call centre agent.

What's next?

Voice biometrics is evolving rapidly, not just in terms of technology but also speed to market. Concepts that were discussed abstractly in academic journals in 2010 were finessed into commercial products by 2011 and are widely used today, such as i-vector factor analysis. There are a few current research areas that could become commercial reality over the next few years.

These include extending the authentication process beyond the initial password-based verification. For example, current systems often use text-dependent (password-based) speaker verification to enable account access. One way to provide additional anti-fraud safeguards is to process the user's subsequent voice samples in text-independent mode. That ensures that the same person is speaking throughout the transaction.

Enabling high accuracy with text-independent voice biometrics and very short utterances is likely to become achievable very soon. One of today's most requested innovations is the ability to authenticate mobile app users or IVR callers with brief phrases that consist of everyday language, such as "Nina, pay my Visa bill."

Today's technology enables accurate authentication using short utterances, but it's text-dependent, meaning users must speak a passphrase such as "My voice is my password." That architecture makes the authentication process overt.

In the near future, biometrics technology will advance to the point where users can be authenticated based on anything they say. That's possible today in the call centre using natural conversation with an agent. After about 10 to 15 seconds, callers can be authenticated with high levels of accuracy. As algorithms improve, the amount of time required will diminish to only a few seconds.

It will also become possible to identify people using only their voice. Today, voice biometrics verifies their identity based on other information they provide, such as their name or account number. Once the system has that identity claim, it can attempt to match the caller's voice with the voiceprint associated with that identity. In the future, callers won't need to provide an identity claim because the system will have the algorithms necessary to compare their voice to all voiceprints in a database.

Combining this ability with text-independent, short-utterance voice biometrics will enable the ideal combination of security, accuracy and user experience. For example, people can simply call their bank, say, "Pay my Visa bill" and the system will know who they are instead of requiring additional validation such as a name or account number.

Although this ideal scenario might seem very far off in the future, it's already common to perform 1-N matching on random speech when searching for fraudsters. The key difference is that today, more utterances are required, and the error rate is such that a human still needs to manually verify the results. Achieving the ideal scenario is simply a matter of improving accuracy.

Multi-factor biometric authentication

Multi-factor authentication will become increasingly prevalent too. Most smartphones and laptops sold over the past few years have a front-facing camera. That installed base creates opportunities to use multiple biometric technologies – voice and facial recognition – simultaneously to enhance security.

As voice biometrics technologies become even more sophisticated, organisations will have ample opportunities to take security and the customer service experience to new heights. The sky is the limit.

About the author

Brett Beranek, solutions marketing manager, Enterprise Marketing, Nuance Communications. He is responsible for solution marketing for Nuance's voice biometric solutions. Prior to joining Nuance, he has held over the past decade various business development and marketing positions within the enterprise B2B security software space. Beranek has extensive experience with biometric technologies, in particular in his role as a founding partner of Viion Systems, a start-up focused on developing facial recognition software solutions for the enterprise market. He also has in-depth experience with a wide range of other security technologies, including fingerprint biometrics, video analytics for the physical security space and license plate recognition technology.